McAfee

wirelesshomenetworksecurity suite

Benutzerhandbuch

McAfee

COPYRIGHT

Copyright © 2005 McAfee, Inc. Alle Rechte vorbehalten. Diese Publikation darf in keiner Form und in keiner Weise ohne die schriftliche Genehmigung von McAfee, Inc., oder ihren Lieferanten und angeschlossenen Unternehmen ganz oder teilweise reproduziert, übertragen, transkribiert, in einem Abrufsystem gespeichert oder in eine andere Sprache übersetzt werden.

MARKEN

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (UND IN KATAKANA), ACTIVESHIELD, ANTIVIRUS ANYWARE UND DESIGN, CLEAN-UP, DESIGN (STILISIERTES E), DESIGN (STILISIERTES N), ENTERCEPT, ENTERPRISE SECURECAST, ENTERPRISE SECURECAST (UND IN KATAKANA), EPOLICY ORCHESTRATOR, FIRST AID, FORCEFIELD, GMT, GROUPSHIELD, GROUPSHIELD (UND IN KATAKANA), GUARD DOG, HOMEGUARD, HUNTER, INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, M UND DESIGN, MCAFEE, MCAFEE (UND IN KATAKANA), MCAFEE UND DESIGN, MCAFEE.COM, MCAFEE VIRUSSCAN, NA NETWORK ASSOCIATES, NET TOOLS, NET TOOLS (UND IN KATAKANA), NETCRYPTO, NETOCTOPUS, NETSCAN, NETSHIELD, NETWORK ASSOCIATES, NETWORK ASSOCIATES COLLISEUM, NETXRAY, NOTESGUARD, NUTS & BOLTS, OIL CHANGE, PC MEDIC, PCNOTARY, PRIMESUPPORT, QUICKCLEAN, RINGFENCE, ROUTER PM, SECURECAST, SECURESELECT, SPAMKILLER, STALKER, THREATSCAN, TIS, TMEG, TOTAL VIRUS DEFENSE, TRUSTED MAIL, UNINSTALLER, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (UND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (UND IN KATAKANA), WEBSTALKER, WEBWALL, WHAT'S THE STATE OF YOUR IDS?, WHO'S WATCHING YOUR NETWORK, YOUR E-BUSINESS DEFENDER, YOUR NETWORK. OUR BUSINESS. sind eingetragene Marken oder Marken von McAfee, Inc. und/oder seinen Tochterunternehmen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind alleiniges Eigentum ihrer jeweiligen Besitzer.

LIZENZINFORMATIONEN

Lizenzvereinbarung

HINWEIS FÜR ALLE BENUTZER: LESEN SIE DEN LIZENZVERTRAG FÜR DIE VON IHNEN ERWORBENE SOFTWARE SORGFÄLTIG DURCH. ER ENTHÄLT DIE ALLGEMEINEN BESTIMMUNGEN UND BEDINGUNGEN FÜR DIE VERWENDUNG DER LIZENZIERTEN SOFTWARE. WENN SIE NICHT WISSEN, WELCHEN SOFTWARE-LIZENZTYP SIE ERWORBEN HABEN, SCHLAGEN SIE IN DEN UNTERLAGEN ZUM KAUF UND WEITEREN UNTERLAGEN BEZÜGLICH DER LIZENZGEWÄHRUNG ODER DER BESTELLUNTERLAGEN NACH, DIE SIE ZUSAMMEN MIT DEM SOFTWAREPAKET ODER SEPARAT (ALS BROSCHÜRE, ALS DATEI AUF DER PRODUKT-CD ODER ALS DATEI VON DER WEBSITE, VON DER SIE AUCH DAS SOFTWAREPAKET HERUNTERGELADEN HABEN) ERHALTEN HABEN. WENN SIE NICHT ALLEN BEDINGUNGEN DIESER VEREINBARUNG ZUSTIMMEN, INSTALLIEREN SIE DIE SOFTWARE NICHT. FALLS ZUTREFFEND, KÖNNEN SIE DAS PRODUKT GEGEN RÜCKERSTATTUNG DES KAUFPREISES AN MCAFEE ODER AN DIE STELLE ZURÜCKGEBEN, AN DER SIE DAS PRODUKT ERWORBEN HABEN.

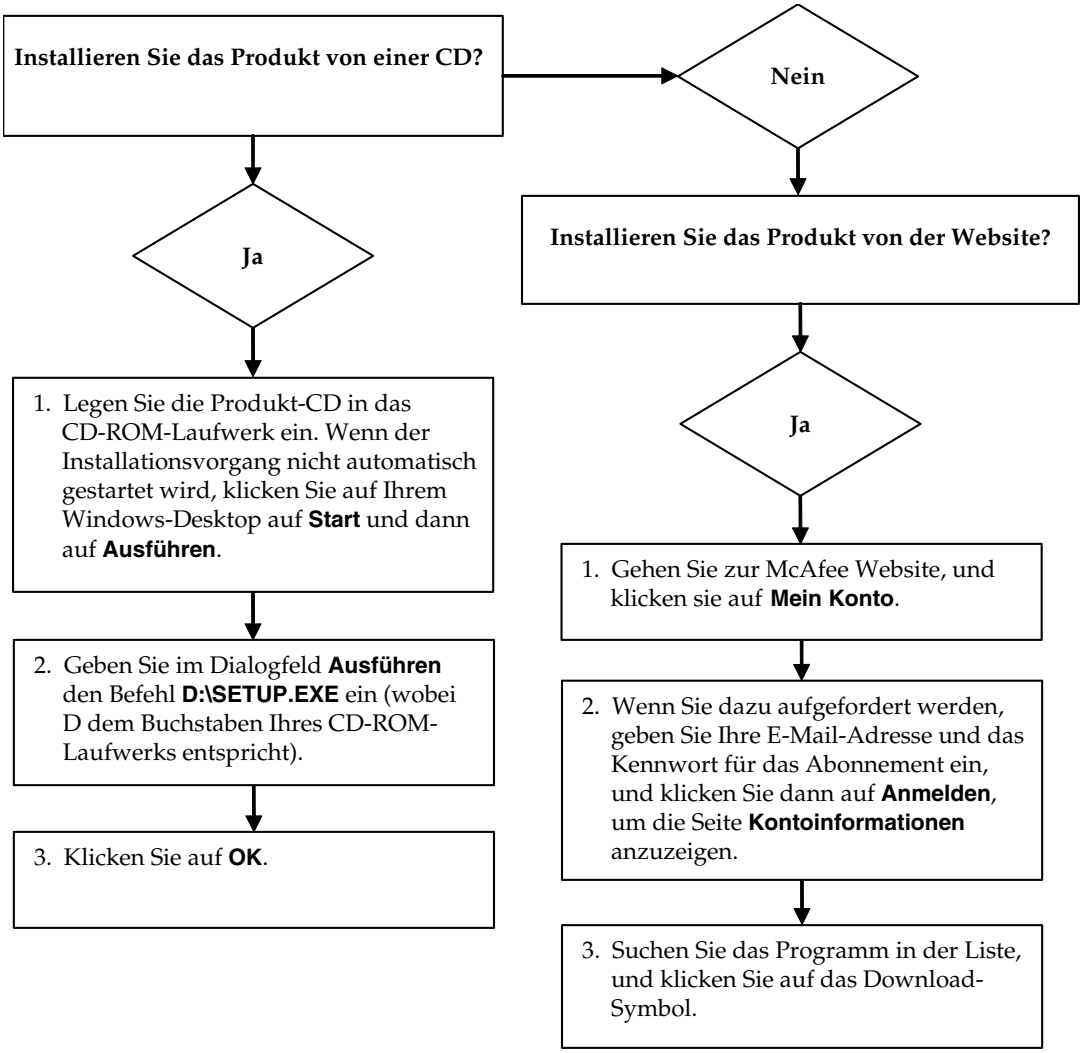
Hinweise

Dieses Produkt enthält oder enthält möglicherweise:

♦ Software, die vom OpenSSL-Projekt zur Verwendung mit dem OpenSSL-Toolkit entwickelt wurde (http://www.openssl.org/). ♦ Kryptographie-Software, die von Eric Young entwickelt wurde, und Software, die von Tim J. Hudson entwickelt wurde. ♦ Softwareprogramme, die gemäß der GNU, General Public License (GPL) oder anderen ähnlichen Lizenzen für kostenlose Software zugelassen werden und es dem Benutzer neben anderen Rechten erlauben, bestimmte Programme oder Teile davon zu kopieren, zu modifizieren und weiterzugeben sowie auf den Quellcode zuzugreifen. Bei Software, die GPL unterliegt und in ausführbarem Binärformat an andere Personen weitergegeben wird, muss diesen Benutzern auch der Quellcode zur Verfügung gestellt werden. Der Quellcode der GPL unterliegenden Software ist auf dieser CD einsehbar. Falls Lizenzen für kostenlose Software verlangen, dass McAfee Rechte für die Nutzung, das Kopieren oder die Modifikation eines Softwareprogramms gewährt, die über die in diesem Vertrag gewährten Rechte hinausgehen, haben Rechte dieser Art Vorrang vor den Rechten und Einschränkungen in diesem Vertrag. ♦ Von Henry Spencer entwickelte Software, Copyright 1992, 1993, 1994, 1997 Henry Spencer. ♦ Von Robert Nordier entwickelte Software, Copyright © 1996-7 Robert Nordier. ♦ Von Douglas W. Sauder entwickelte Software. ♦ Von der Apache Software Foundation entwickelte Software (http://www.apache.org/). Eine Kopie der Lizenzvereinbarung für diese Software finden Sie unter www.apache.org/licenses/LICENSE-2.0.txt. ♦ International Components for Unicode ("ICU") Copyright © 1995-2002 International Business Machines Corporation und andere. ♦ Software, die von CrystalClear Software, Inc., entwickelt wurde, Copyright © 2000 CrystalClear Software, Inc., ♦ FEAD® Optimizer®-Technologie, Copyright Netopsystems AG, Berlin, Deutschland. ♦ Outside In® Viewer Technology © 1992-2001 Stellent Chicago, Inc., und/oder Outside In® HTML Export, © 2001 Stellent Chicago, Inc., ♦ Software, urheberrechtlich geschützt von Thai Open Source Software Center Ltd. und Clark Cooper, © 1998, 1999, 2000. ♦ Software, urheberrechtlich geschützt von Expat maintainers. ♦ Software, urheberrechtlich geschützt von The Regents of the University of California, © 1989. ♦ Software, urheberrechtlich geschützt von Gunnar Ritter. ♦ Software, urheberrechtlich geschützt von Sun Microsystems®, Inc., © 2003. ♦ Software, urheberrechtlich geschützt von Gisle Aas. © 1995-2003. ♦ Software, urheberrechtlich geschützt von Michael A. Chase, © 1999-2000. ♦ Software, urheberrechtlich geschützt von Neil Winton, © 1995-1996. ♦ Software, urheberrechtlich geschützt von RSA Data Security, Inc., © 1990-1992. ♦ Software, urheberrechtlich geschützt von Sean M. Burke, © 1999, 2000. ♦ Software, urheberrechtlich geschützt von Martijn Koster, © 1995. ♦ Software, urheberrechtlich geschützt von Brad Appleton, © 1996-1999. ♦ Software, urheberrechtlich geschützt von Michael G. Schwern, © 2001. ♦ Software, urheberrechtlich geschützt von Graham Barr, © 1998. ♦ Software, urheberrechtlich geschützt von Larry Wall und Clark Cooper, © 1998-2000. ♦ Software, urheberrechtlich geschützt von Frodo Looijaard, © 1997. ♦ Software, urheberrechtlich geschützt von Python Software Foundation, Copyright © 2001, 2002, 2003. Eine Kopie des Lizenzvertrags für diese Software erhalten Sie unter www.python.org. ♦ Software, urheberrechtlich geschützt von Beman Dawes, © 1994-1999, 2002. ♦ Von Andrew Lumsdaine entwickelte Software, Lie-Quan Lee, Jeremy G. Siek © 1997-2000 University of Notre Dame. ♦ Software, urheberrechtlich geschützt von Simone Bordet & Marco Cravero, © 2002. ♦ Software, urheberrechtlich geschützt von Stephen Purcell, © 2001. ♦ Software, urheberrechtlich geschützt von Indiana University Extreme! Lab entwickelte Software (http://www.extreme.indiana.edu/). ♦ Software, urheberrechtlich geschützt von International Business Machines Corporation und anderen, © 1995-2003. ♦ Von der University of California, Berkeley und deren Mitwirkenden entwickelte Software. ♦ Von Ralf S. Engelschall, <rse@engelschall.com>, entwickelte Software für die Verwendung im mod_ssl-Projekt (http://www.modssl.org/). ♦ Software, urheberrechtlich geschützt von Kevlin Henney, © 2000-2002. ♦ Software, urheberrechtlich geschützt von Peter Dimov und Multi Media Ltd. © 2001, 2002. ♦ Software, urheberrechtlich geschützt von David Abrahams, © 2001, 2002. Dokumentation dazu finden Sie unter http://www.boost.org/libs/bind/bind.html. ♦ Software, urheberrechtlich geschützt von Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, © 2000. ♦ Software, urheberrechtlich geschützt von Boost.org, © 1999-2002. ♦ Software, urheberrechtlich geschützt von Nicolai M. Josuttis, © 1999. ♦ Software, urheberrechtlich geschützt von Jeremy Siek, © 1999-2001. ♦ Software, urheberrechtlich geschützt von Daryle Walker, © 2001. ♦ Software, urheberrechtlich geschützt von Chuck Allison und Jeremy Siek, © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Samuel Krempp, © 2001. Aktualisierungen, Dokumentation und Versionsverlauf dazu finden Sie unter http://www.boost.org. ♦ Software, urheberrechtlich geschützt von Doug Gregor (gregod@cs.rpi.edu), © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Cadenza New Zealand Ltd., © 2000. ♦ Software, urheberrechtlich geschützt von Jens Maurer, © 2000, 2001. ♦ Software, urheberrechtlich geschützt von Jaakko Järvi (jaakko.jarvi@cs.utu.fi), © 1999, 2000. ♦ Software, urheberrechtlich geschützt von Ronald Garcia, © 2002. ♦ Software, urheberrechtlich geschützt von David Abrahams, Jeremy Siek und Daryle Walker, © 1999-2001. ♦ Software, urheberrechtlich geschützt von Stephen Cleary (shammah@voyager.net), © 2000. ♦ Software, urheberrechtlich geschützt von Housemarque Oy <http://www.housemarque.com>, © 2001. ♦ Software, urheberrechtlich geschützt von Paul Moore, © 1999. ♦ Software, urheberrechtlich geschützt von Dr. John Maddock, © 1998-2002. ♦ Software, urheberrechtlich geschützt von Greg Colvin und Beman Dawes, © 1998, 1999. ♦ Software, urheberrechtlich geschützt von Peter Dimov, © 2001, 2002. ♦ Software, urheberrechtlich geschützt von Jeremy Siek und John R. Bandela, © 2001. ♦ Software, urheberrechtlich geschützt von Joerg Walter und Mathias Koch, © 2000-2002.

Schnellreferenz

Wenn Sie das Produkt von einer CD oder einer Website aus installieren, sollten Sie diese praktische Referenzseite ausdrucken.


Installieren Sie das Produkt von einer CD?
Ja
1. Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein. Wenn der Installationsvorgang nicht automatisch gestartet wird, klicken Sie auf Ihrem Windows-Desktop auf **Start** und dann auf **Ausführen**.
2. Geben Sie im Dialogfeld **Ausführen** den Befehl **D:\SETUP.EXE** ein (wobei D dem Buchstaben Ihres CD-ROM-Laufwerks entspricht).
3. Klicken Sie auf **OK**.
Nein
Installieren Sie das Produkt von der Website?
Ja
1. Gehen Sie zur McAfee Website, und klicken sie auf **Mein Konto**.
2. Wenn Sie dazu aufgefordert werden, geben Sie Ihre E-Mail-Adresse und das Kennwort für das Abonnement ein, und klicken Sie dann auf **Anmelden**, um die Seite **Kontoinformationen** anzuzeigen.
3. Suchen Sie das Programm in der Liste, und klicken Sie auf das Download-Symbol.

McAfee behält sich das Recht vor, Upgrade- und Support-Pläne sowie Richtlinien jederzeit ohne Ankündigung zu ändern. McAfee und seine Produktnamen sind eingetragene Marken von McAfee, Inc. und/oder von seinen Tochterunternehmen in den USA und/oder anderen Ländern.
© 2005 McAfee, Inc. Alle Rechte vorbehalten.

Weitere Informationen

Zum Anzeigen der Benutzerhandbücher auf der Produkt-CD muss Acrobat Reader installiert sein. Andernfalls installieren Sie das Programm jetzt von der McAfee-Produkt-CD.

1. Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein.
2. Öffnen Sie Windows-Explorer: Klicken Sie auf dem Windows-Desktop auf **Start** und dann auf **Suchen**.
3. Suchen Sie den Ordner mit den Handbüchern (Manuals), und doppelklicken Sie auf die PDF-Datei des Benutzerhandbuchs, das Sie öffnen möchten.

Registrierungsvorteile

Es wird empfohlen, die im Produkt beschriebenen, einfachen Schritte zu befolgen, um Ihre Registrierung direkt an uns zu senden. Durch die Registrierung wird sichergestellt, dass Ihnen im angemessenen Zeitrahmen professionelle technische Unterstützung zur Verfügung steht. Weitere Vorteile sind:

- KOSTENLOSER elektronischer Support
- Updates für Virusdefinitionsdateien (DAT-Dateien) für ein Jahr ab dem Zeitpunkt der Installation beim Kauf der VirusScan-Software

  Preisangaben für ein zusätzliches Jahr Virussignaturen erhalten Sie unter http://de.mcafee.com/.
- Umtauschgarantie von 60 Tagen für Ihre Software-CD, falls diese fehlerhaft oder beschädigt ist
- SpamKiller-Filter-Updates für ein Jahr ab dem Zeitpunkt der Installation bei Kauf der SpamKiller-Software

  Preisangaben für ein zusätzliches Jahr Filter-Updates erhalten Sie unter http://de.mcafee.com/.
- McAfee Internet Security Suite-Updates für ein Jahr ab dem Zeitpunkt der Installation bei Kauf der MIS-Software

  Preisangaben für ein zusätzliches Jahr Inhalts-Updates erhalten Sie unter http://de.mcafee.com/.

Technischer Support

Technischen Support erhalten Sie unter http://www.mcafeehilfe.com/.

Unsere Support-Site ermöglicht Ihnen rund um die Uhr den Zugriff auf einen benutzerfreundlichen Antwort-Assistenten, der Ihnen Antworten auf die häufigsten Fragen gibt.

Für erfahrene Benutzer stehen außerdem erweiterte Optionen zur Verfügung, zum Beispiel eine Schlüsselwortsuche und unsere strukturierte Hilfe. Wenn sich keine Lösung findet, können Sie außerdem KOSTENLOS auf unsere Dienste Chat Now! und E-Mail Express! zugreifen. Per Chat und E-Mail können Sie über das Internet schnell einen qualifizierten Support-Mitarbeiter erreichen, wobei Ihnen keine Kosten entstehen. Außerdem gibt es noch die Möglichkeit von telefonischem Support, über den Sie hier mehr Informationen finden können: http://www.mcafeehilfe.com/.

Inhalt

Schnellreferenz iii

1 Erste Schritte 9

Systemanforderungen 9
Verwenden von McAfee SecurityCenter 11

2 McAfee Wireless Home Network Security 13

Verwenden von McAfee Wireless Home Network Security 13
Schützen Ihres Netzwerks 13
Grundlegendes zu Wireless Home Network Security 14
Wireless Home Network Security macht Ihnen die Arbeit leicht 15
Funktionen 16
Installieren von Wireless Home Network Security 17
Installieren von einer CD 17
Installieren von der Website 17
Installieren mithilfe der Installationsdatei 18
Verwenden des Konfigurationsassistenten 18
Verwenden der Seite "Zusammenfassung" 19
Anzeigen Ihrer Verbindung 19
Anzeigen Ihres geschützten drahtlosen Netzwerks 20
Verwalten drahtloser Netzwerke 21
Verbinden mit einem Netzwerk 22
Trennen einer Netzwerkverbindung 22
Verwenden erweiterter Optionen 22
Konfigurieren von Optionen 23
Anzeigen von Ereignissen 24
Konfigurieren erweiterter Einstellungen 24
Konfigurieren von Sicherheitseinstellungen 24
Konfigurieren von Warnungseinstellungen 25
Konfigurieren weiterer Einstellungen 25
Widerrufen des Zugriffs auf das Netzwerk 26
Reparieren von Sicherheitseinstellungen 26
Schützen anderer Computer 27

Rotieren des Schlüssels 28
Schützen drahtloser Netzwerke 28
Aufheben des Schutzes drahtloser Netzwerke 28
Aktualisieren von Wireless Home Network Security 28
Automatisches Prüfen auf Updates 29
Manuelles Prüfen auf Updates 29
Grundlegendes zu Warnungen 30
Computer gesichert 30
Computer getrennt 30
Computer verbunden 30
Drahtloser Router/Zugriffspunkt geschützt 30
Fehler bei der Schlüsselrotation 30
Häufigkeit der Sicherheitsschlüsselrotation geändert 31
Kennwort geändert 31
Netzwerk repariert 31
Netzwerk umbenannt 31
Netzwerkeinstellungen geändert 31
Netzwerkkonfiguration geändert 31
Schlüsselrotation ausgesetzt 32
Schlüsselrotation fortgesetzt 32
Schutz für drahtlosen Router/Zugriffspunkt aufgehoben 32
Sicherheitsschlüssel rotiert 32
Zugriff widerrufen 32
Problembehandlung 33
Installation 33
Auf welchen Computern muss diese Software installiert werden? 33
Drahtloser Adapter wird nicht erkannt 33
Mehrere drahtlose Adapter 33
Kein Download auf drahtlose Computer möglich, da das Netzwerk bereits sicher ist 34
Schützen oder Konfigurieren des Netzwerks 34
Nicht unterstützter Router oder Zugriffspunkt 34
Aktualisieren der Firmware des Routers oder Zugriffspunktes 35
Fehler durch doppelte Administratoren 35
Netzwerk als ungesichert angezeigt 35
Keine Reparatur möglich 35
Verbinden von Computern mit Ihrem Netzwerk 36
Warten auf Autorisierung 36
Gewähren von Zugriff für einen unbekannten Computer 36

Verbinden mit einem Netzwerk oder dem Internet 37
Schlechte Verbindung zum Internet 37
Kurze Unterbrechung der Verbindung 37
Verbindungsverlust bei Geräten (nicht beim Computer) 37
Aufforderung zur Eingabe des WEP- oder WPA-Schlüssels 37
Keine Verbindung möglich 38
Aktualisieren des drahtlosen Adapters 38
Schwaches Signal 39
Windows kann die drahtlose Verbindung nicht konfigurieren 40
Windows zeigt keine Verbindung an 40
Andere Probleme 40
Bei Verwendung anderer Programme lautet der Netzwerkname anders 40
Probleme beim Konfigurieren drahtloser Router oder Zugriffspunkte 40
Ersetzen von Computern 42
Software funktioniert nach dem Aktualisieren des Betriebssystems nicht 42
Glossar 42

3 McAfee VirusScan 53

Neue Funktionen 53
Testen von VirusScan 54
Testen von ActiveShield 54
Testen von Scan 55
Verwenden von McAfee VirusScan 56
Verwenden von ActiveShield 57
Aktivieren oder Deaktivieren von ActiveShield 57
Konfigurieren von ActiveShield-Optionen 58
Grundlegendes zu Sicherheitswarnungen 68
Manuelles Überprüfen des Computers 71
Manuelles Prüfen auf Viren und andere Bedrohungen 71
Automatisches Überprüfen auf Viren und andere Bedrohungen 76
Grundlegendes zu Bedrohungserkennungen 78
Verwalten von isolierten Dateien 80
Erstellen einer Rettungsdiskette 82
Einrichten des Schreibschutzes für eine Rettungsdiskette 83
Verwenden einer Rettungsdiskette 83
Aktualisieren einer Rettungsdiskette 84

Automatisches Melden von Viren 84
Melden von Vireninformationen an die World Virus Map 84
Anzeigen der World Virus Map 86
Aktualisieren von VirusScan 87
Automatisches Prüfen auf Updates 87
Manuelles Prüfen auf Updates 87

4 McAfee Personal Firewall Plus 89

Neue Funktionen 89
Deinstallieren anderer Firewalls 91
Festlegen der Standard-Firewall 92
Festlegen der Sicherheitsstufe 92
Testen von McAfee Personal Firewall Plus 95
Verwenden von McAfee Personal Firewall Plus 95
Informationen zur Seite "Zusammenfassung" 95
Informationen zur Seite "Internetanwendungen" 101
Ändern von Anwendungsregeln 102
Zulassen und Blockieren von Internetanwendungen 102
Informationen zur Seite "Eingehende Ereignisse" 103
Grundlegendes zu Ereignissen 104
Anzeigen von Ereignissen im Protokoll für eingehende Ereignisse 107
Reagieren auf eingehende Ereignisse 109
Verwalten des Protokolls eingehender Ereignisse 113
Informationen zu Warnungen 115
Rote Warnmeldungen 115
Grüne Warnungen 121
Blaue Warnungen 122

Index 125

Erste Schritte 1

Das Internet bietet eine Fülle an Informationen und Unterhaltung. Sobald Sie aber eine Internetverbindung herstellen, sind Ihr Computer, Ihre Daten und Ihr drahtloses Netzwerk einer Vielzahl von Sicherheitsrisiken und -bedrohungen ausgesetzt. Schützen Sie deshalb Ihr drahtloses Netzwerk, Ihren Computer und Ihre Daten mit der McAfee Wireless Home Network Security Suite. Mit den preisgekrönten Technologien, die in McAfee Wireless Home Network Security, McAfee VirusScan und McAfee Personal Firewall Plus enthalten sind, stellt die Wireless Home Network Security Suite eine der umfassendsten derzeit erhältlichen Zusammenstellungen von Datenschutz- und Sicherheits-Tools dar.

Wenn Sie mehr über die einzelnen McAfee-Produkte erfahren möchten, lesen Sie bitte die folgenden Kapitel:

- *McAfee Wireless Home Network Security* auf Seite 13
- *McAfee VirusScan* auf Seite 53
- *McAfee Personal Firewall Plus* auf Seite 89

Systemanforderungen

- Microsoft® Windows 98SE, Windows Me, Windows 2000 oder Windows XP
- PC mit Pentium-kompatiblem Prozessor

  Windows 98 oder Windows 2000: 133 MHz oder höher

  Windows Me: 150 MHz oder höher

  Windows XP (Home und Professional): 300 MHz oder höher
- RAM

  Windows 98SE, Me oder 2000: 64 MB

  Windows XP (Home und Professional): 128 MB
- 100 MB Festplattenspeicher
- Microsoft Internet Explorer 5.5 oder höher

HINWEIS
Sie können die neueste Version von Internet Explorer von der Microsoft-Website unter http://www.microsoft.com/ herunterladen.

Drahtloses Netzwerk

- Herkömmlicher drahtloser Netzwerkadapter
- Herkömmlicher drahtloser Router oder Zugriffspunkt, darunter die meisten Modelle von Linksys®, NETGEAR®, D-Link® und Belkin®

Unterstützte E-Mail-Programme

- POP3 (Outlook Express, Outlook, Eudora, Netscape)

Unterstützte Instant Messaging-Programme

- AOL Instant Messenger 2.1 oder höher
- Yahoo Messenger 4.1 oder höher
- Microsoft Windows Messenger 3.6 oder höher
- MSN Messenger 6.0 oder höher

Verwenden von McAfee SecurityCenter

McAfee SecurityCenter ist Ihre Anlaufstelle für alle Sicherheitsbelange. Durch die nahtlose Integration in McAfee SecurityCenter erhalten Sie einen fundierten Überblick über den Sicherheitsstatus Ihres Computers zuzüglich der neuesten Sicherheits- und Virenwarnungen. Sie können SecurityCenter mithilfe des McAfee-Symbols in der Windows-Taskleiste oder vom Windows-Desktop aus starten.

HINWEIS
Wenn Sie weitere Informationen zu den Funktionen anzeigen möchten, klicken Sie im Dialogfenster **SecurityCenter** auf **Hilfe**.

Wenn SecurityCenter ausgeführt wird und sämtliche auf Ihrem Computer installierten McAfee-Funktionen aktiviert sind, wird in der Windows-Taskleiste (Windows XP-Infobereich) ein rotes **M**-Symbol angezeigt.

Wenn eine oder mehrere der installierten McAfee-Anwendungen deaktiviert sind, ändert sich die Farbe des McAfee-Symbols zu schwarz: .

So öffnen Sie McAfee SecurityCenter:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol .
2. Klicken Sie auf **SecurityCenter öffnen**.

So greifen Sie auf ein McAfee-Produkt zu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol .
2. Zeigen Sie auf das entsprechende McAfee-Produkt, und klicken Sie dann auf die Funktion, die Sie verwenden möchten.

McAfee Wireless Home Network Security 2

Willkommen bei McAfee Wireless Home Network Security. Dieses Programm bietet umfassenden Schutz für Ihr drahtloses Netzwerk, Ihre persönlichen Daten und Ihren Computer.

Das Programm ist für Computer mit drahtlosen Verbindungen ausgelegt. Wenn Sie es auf Computern installieren, die per Kabel mit Ihrem Netzwerk verbunden sind, steht auf den verkabelten Computern nicht der volle Funktionsumfang zur Verfügung.

Durch Verschlüsselung Ihrer persönlichen, privaten Daten bei der Übertragung sorgt McAfee Wireless Home Network Security für optimalen Datenschutz in Ihrem geschützten drahtlosen Netzwerk und verhindert, dass Hacker auf Ihre Informationen zugreifen.

Verwenden von McAfee Wireless Home Network Security

Beachten Sie Folgendes, bevor Sie Ihr Netzwerk schützen.

- Kabelverbindungen – Computer, die per Kabel mit dem Router verbunden sind, müssen nicht geschützt werden, da per Kabel übertragene Signale nicht abgefangen werden können.
- Drahtlose Verbindungen – Computer mit drahtloser Verbindung sollten geschützt werden, da ihre Daten abgefangen werden können. Ein Netzwerk muss mithilfe eines drahtlosen Computers geschützt werden, denn nur ein drahtloser Computer kann einem anderen drahtlosen Computer Zugriff gewähren.

Schützen Ihres Netzwerks

Bei einer kabelgebundenen Verbindung müssen Sie das Netzwerk nicht schützen.

1. Installieren Sie auf Ihrem drahtlosen Computer den drahtlosen Adapter, und aktivieren Sie ihn. Der drahtlose Adapter kann eine Karte sein, die seitlich im Computer eingesteckt ist, oder er kann am USB-Anschluss angeschlossen sein. Viele neuere Computer sind mit einem integrierten Drahtlosadapter ausgerüstet, so dass Sie keinen installieren müssen.

2 Installieren Sie Ihren drahtlosen Router oder Zugriffspunkt (mithilfe von Zugriffspunkten wird die Reichweite erweitert), und stellen Sie sicher, dass er eingeschaltet und aktiviert ist. Eine umfassendere Definition eines Routers und Zugriffspunktes finden Sie im *Glossar* auf Seite 42.

3 Installieren Sie McAfee Wireless Home Network Security auf allen drahtlosen Computern im Netzwerk. Auf Computern, die per Kabel verbunden sind, müssen Sie die Software nicht installieren. Siehe *Installieren von Wireless Home Network Security* auf Seite 17.

4 Schützen Sie das Netzwerk von einem der drahtlosen Computer aus. Siehe *Schützen drahtloser Netzwerke* auf Seite 28.

5 Melden Sie sich von den anderen drahtlosen Computern aus am Netzwerk an. Siehe *Schützen anderer Computer* auf Seite 27.

Grundlegendes zu Wireless Home Network Security

Wie viele andere auch, nutzen Sie zu Hause ein drahtloses Netzwerk, weil es einfach und bequem ist. Mit einem solchen Netzwerk haben Sie in jedem Zimmer und sogar im Garten Zugang zum Internet – ohne die Kosten und Probleme, die mit Kabeln verbunden sind. Dank der Drahtlostechnik können Sie Angehörigen und Freunden ganz einfach den Zugriff auf das Netzwerk ermöglichen.

Allerdings ist diese Bequemlichkeit mit einigen Sicherheitsrisiken verbunden. In drahtlosen Netzwerken werden die Daten per Funk übertragen, und diese Funksignale machen an den Wänden Ihrer Wohnung nicht halt. Mit speziellen Antennen können Unbefugte auf Ihr drahtloses Netzwerk zugreifen und Ihre Daten noch aus mehreren Kilometern Entfernung abfangen.

Zum Schutz Ihres drahtlosen Netzwerks und Ihrer Daten müssen Sie den Zugriff auf das Netzwerk beschränken und die Daten verschlüsseln. Zwar sind in Ihrem drahtlosen Router oder Zugriffspunkt Sicherheitsstandards integriert, doch besteht die Schwierigkeit darin, die Sicherheitseinstellungen richtig zu aktivieren und zu verwalten. Mehr als 60 Prozent aller drahtlosen Netzwerke sind nicht in einem ausreichend hohen Maße (etwa durch Verschlüsselung) geschützt.

Wireless Home Network Security macht Ihnen die Arbeit leicht

McAfee Wireless Home Network Security aktiviert die Sicherheitseinstellungen in Ihrem drahtlosen Netzwerk und schützt die übertragenen Daten mit einem einfachen, mit einem Klick zu bewältigenden Vorgang, bei dem automatisch ein starker Verschlüsselungsschlüssel generiert wird. Die meisten Schlüssel, die für Nutzer leicht zu merken sind, können von Hackern mühelos geknackt werden. Indem sich der Computer den Schlüssel für Sie "merkt", kann Wireless Home Network Security Schlüssel verwenden, die fast unmöglich zu knacken sind.

Außerdem generiert und verteilt diese Software, während sie unauffällig im Hintergrund ausgeführt wird, alle paar Minuten einen neuen Verschlüsselungsschlüssel, so dass selbst der entschlossenste Hacker aufgeben muss. Berechtigte Computer, etwa jene von Familienangehörigen und Freunden, die auf das drahtlose Netzwerk zugreifen möchten, erhalten den starken Verschlüsselungsschlüssel sowie alle verteilten Schlüssel.

Diese Lösung bietet umfassende Sicherheit und kann dennoch mühelos vom Besitzer eines drahtlosen Netzwerks zu Hause implementiert werden. Mit einem Klick können Sie Hacker davon abhalten, Ihre drahtlos übertragenen Daten zu stehlen. Hacker können keine Trojaner oder andere bösartige Programme in Ihr Netzwerk einschleusen. Sie können Ihr drahtloses Netzwerk auch nicht als Ausgangspunkt für Spam- oder Virenangriffe missbrauchen. Selbst Gelegenheits-Freeloader können nicht auf das drahtlose Netzwerk zugreifen; dadurch können Sie auch nicht irrtümlich für illegale Film- oder Musik-Downloads angeklagt werden.

Andere Lösungen bieten weder die Einfachheit noch die umfassende Sicherheit von Wireless Home Network Security. Das Filtern von MAC-Adressen oder das Deaktivieren der SSID-Übertragung gewährt nur oberflächlichen Schutz. Selbst unerfahrene Hacker können diese Mechanismen mit frei erhältlichen Tools aus dem Internet umgehen. Andere Hilfsmittel wie VPNs schützen nicht das drahtlose Netzwerk an sich, somit ist es nach wie vor anfällig für eine Vielzahl von Angriffen.

McAfee Wireless Home Network Security ist das erste Programm, das Ihr drahtloses Heimnetzwerk wirklich umfassend absichert.

Funktionen

Diese Version von Wireless Home Network Security bietet die folgenden Funktionen:

- Ständig aktiver Schutz – Erkennt und schützt automatisch gefährdete drahtlose Netzwerke, zu denen Sie eine Verbindung herstellen.
- Leicht verständliche Benutzeroberfläche – Ermöglicht Ihnen den Schutz des Netzwerks, ohne dass Sie schwierige Entscheidungen treffen oder komplizierte technische Begriffe kennen müssen.
- Starke automatische Verschlüsselung – Gewährt ausschließlich Familienangehörigen und Freunden Zugriff auf das Netzwerk und schützt Ihre Daten bei der Übertragung.
- Reine Softwarelösung – Wireless Home Network Security funktioniert mit einem herkömmlichen drahtlosen Router oder Zugriffspunkt und mit normaler Sicherheitssoftware. Sie müssen keine zusätzliche Hardware erwerben.
- Automatische Schlüsselrotation – Selbst die entschlossensten Hacker können Ihre Daten nicht abfangen, da der Schlüssel ständig geändert wird.
- Hinzufügen von Netzwerkbenutzern – Sie können Ihren Familienangehörigen und Freunden mühelos Zugriff auf das Netzwerk gewähren.
- Intuitives Verbindungs-Tool – Das Tool für drahtlose Verbindungen ist intuitiv zu bedienen und informativ. Es zeigt Details zur Signalstärke und zum Sicherheitsstatus an.
- Ereignisprotokollierung und Warnungen – Leicht verständliche Berichte und Warnungen bieten erfahrenen Benutzern weitere Informationen zum drahtlosen Netzwerk.
- Aussetzmodus – Hiermit können Sie die Schlüsselrotation vorübergehend aussetzen, damit bestimmte Anwendungen ohne Unterbrechung ausgeführt werden können.
- Kompatibilität mit anderer Hardware – Wireless Home Network Security aktualisiert sich selbst automatisch mit den neuesten Modulen für drahtlose Router oder Zugriffspunkte der am häufigsten verwendeten Marken. Dazu gehören: Linksys®, NETGEAR®, D-Link®, Belkin® und andere.

Installieren von Wireless Home Network Security

In diesem Kapitel werden die Installation von Wireless Home Network Security und die ersten Schritte zum Schützen Ihres Netzwerks beschrieben.

Achten Sie beim Installieren von Wireless Home Network Security auf Folgendes.

- Installieren Sie die Software auf allen drahtlosen Computern.
- Auf Computern, die per Kabel verbunden sind, müssen Sie die Software nicht installieren.

Installieren von einer CD

1. Legen Sie die Produkt-CD in das CD-ROM-Laufwerk ein. Wenn der Installationsvorgang nicht automatisch gestartet wird, klicken Sie auf Ihrem Windows-Desktop auf **Start** und dann auf **Ausführen**.
2. Geben Sie im Dialogfeld **Ausführen** den Befehl D:\SETUP.EXE ein (wobei D dem Buchstaben Ihres CD-ROM-Laufwerks entspricht).
3. Klicken Sie auf **OK**.
4. Gehen Sie zu *Verwenden des Konfigurationsassistenten* auf Seite 18.

Installieren von der Website

Wenn Sie Wireless Home Network Security von der Website aus installieren, müssen Sie die Installationsdatei speichern. Mithilfe dieser Datei wird Wireless Home Network Security auf anderen Computern installiert.

1. Gehen Sie zur McAfee Website, und klicken sie auf **Mein Konto**.
2. Wenn Sie dazu aufgefordert werden, geben Sie die E-Mail-Adresse und das Kennwort für das Abonnement ein, und klicken Sie dann auf **Anmelden**, um die Seite **Kontoinformationen** anzuzeigen.
3. Suchen Sie Ihr Programm in der Liste, und klicken Sie auf **Ziel speichern unter**. Die Installationsdatei wird auf Ihrem Computer gespeichert.

Installieren mithilfe der Installationsdatei

Wenn Sie das Installationspaket heruntergeladen haben (also über keine CD verfügen), müssen Sie die Software auf allen drahtlosen Computern installieren. Nachdem das Netzwerk geschützt worden ist, kann mit drahtlosen Computern ohne Eingabe des Schlüssels keine Verbindung zum Netzwerk hergestellt werden. Führen Sie einen der folgenden Schritte aus:

- Laden Sie das Installationspaket auf alle drahtlosen Computer herunter, bevor Sie das Netzwerk schützen.
- Kopieren Sie die Installationsdatei auf einen USB-Speicherstick oder eine beschreibbare CD, und installieren Sie die Software auf den anderen drahtlosen Computern.
- Schließen Sie, falls das Netzwerk bereits geschützt ist, ein Kabel am Router an, um die Datei herunterzuladen. Sie können auch auf **Aktuellen Schlüssel anzeigen** klicken, um den aktuellen Schlüssel anzuzeigen und damit eine Verbindung zum drahtlosen Netzwerk herzustellen.

Befolgen Sie nach der Installation von Wireless Home Network Security auf allen drahtlosen Computern die Anweisungen auf dem Bildschirm. Wenn Sie auf **Fertig stellen** klicken, wird der Konfigurationsassistent geöffnet. Gehen Sie zu *Verwenden des Konfigurationsassistenten*.

Verwenden des Konfigurationsassistenten

Mit dem Konfigurationsassistenten können Sie die folgenden Aufgaben ausführen:

- Schützen des Netzwerks von einem der drahtlosen Computer aus. Weitere Informationen finden Sie unter *Schützen drahtloser Netzwerke* auf Seite 28.

  Wenn Wireless Home Network Security den richtigen zu schützenden Router oder Zugriffspunkt nicht ermitteln kann, werden Sie aufgefordert, den Vorgang zu wiederholen oder abzubrechen. Rücken Sie näher an den Router bzw. Zugriffspunkt heran, den Sie schützen möchten, und klicken Sie dann auf **Wiederholen**.
- Anmelden an einem geschützten Netzwerk (bei Vorhandensein von nur einem drahtlosen Computer ist dieser Schritt nicht erforderlich). Weitere Informationen finden Sie unter *Verwalten drahtloser Netzwerke* auf Seite 21.
- Herstellen einer Verbindung zu einem Netzwerk. Weitere Informationen finden Sie unter *Verbinden mit einem Netzwerk* auf Seite 22.

Falls der drahtlose Adapter nicht erkannt wird oder der drahtlose Router oder Zugriffspunkt nicht eingeschaltet ist, werden Sie benachrichtigt.

Verwenden der Seite "Zusammenfassung"

Wenn Sie den Status Ihrer Verbindung anzeigen möchten, klicken Sie mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie **Zusammenfassung** aus. Die Seite **Zusammenfassung** wird angezeigt (Abbildung 2-1).

Abbildung 2-1. Seite "Zusammenfassung"

Anzeigen Ihrer Verbindung

Der Fensterbereich **Verbindung** zeigt den Status Ihrer Verbindung an. Wenn Sie eine Überprüfung Ihrer drahtlosen Verbindung durchführen möchten, klicken Sie auf **Sicherheitsscan**.

- Status – Zeigt an, ob Sie verbunden oder getrennt sind. Wenn Sie verbunden sind, wird der Name des Netzwerks angezeigt.
- Sicherheit – Der Sicherheitsmodus des Netzwerks.
- Geschwindigkeit – Die Verbindungsgeschwindigkeit Ihrer drahtlosen Netzwerkkarte.
- Dauer – Die Dauer Ihrer Verbindung zu diesem Netzwerk.
- Signalstärke – Die Stärke des Signals der drahtlosen Verbindung.

Anzeigen Ihres geschützten drahtlosen Netzwerks

Der Fensterbereich **Geschütztes drahtloses Netzwerk** enthält Informationen zu Ihrem Netzwerk.

- Verbindungen heute – Gibt an, wie oft Benutzer am aktuellen Tag eine Verbindung zu diesem Netzwerk hergestellt haben.
- Schlüsselrotationen heute – Gibt an, wie oft der Schlüssel am aktuellen Tag geändert wurde, einschließlich der Zeit seit der letzten Änderung.
- Schlüsselrotation ausgesetzt – Die Schlüsselrotation in Ihrem Netzwerk ist ausgesetzt. Klicken Sie auf **Schlüsselrotation fortsetzen**, um die Rotation fortzusetzen und sicherzustellen, dass das Netzwerk vollständig vor Hackern geschützt ist.
- In diesem Monat gesicherte Computer – Gibt an, wie viele Computer im laufenden Monat gesichert wurden.
- Computer – Wenn Sie mit einem geschützten Netzwerk verbunden sind, werden alle im Netzwerk befindlichen Computer sowie der Zeitpunkt angezeigt, zu dem diese jeweils zum letzten Mal verbunden waren.

  – Der Computer ist verbunden.

  – Der Computer kann ohne Anmeldung am Netzwerk erneut eine Verbindung herstellen.

  – Der Computer ist nicht verbunden. Der Computer muss sich am Netzwerk neu anmelden, weil der Schlüssel aktualisiert wurde.

Klicken Sie auf **Netzwerkereignisse anzeigen**, um Netzwerkereignisse anzuzeigen. Siehe *Anzeigen von Ereignissen* auf Seite 24.

Klicken Sie auf **Aktuellen Schlüssel anzeigen**, um den Schlüssel anzuzeigen.

Wenn Sie drahtlose Geräte, die von Wireless Home Network Security nicht unterstützt werden, mit dem Netzwerk verbinden (z. B. einen Handheld), gehen Sie folgendermaßen vor.

1. Klicken Sie zum Anzeigen dieser Protokolle auf **Netzwerkereignisse anzeigen**.
2. Notieren Sie den Schlüssel.
3. Klicken Sie auf **Schlüsselrotation aussetzen**. Durch Aussetzen der Schlüsselrotation wird verhindert, dass die Verbindung zu manuell mit dem Netzwerk verbundenen Geräten getrennt wird.
4. Geben Sie den Schlüssel im Gerät ein.

Klicken Sie auf **Schlüsselrotation fortsetzen**, wenn Sie diese Geräte nicht mehr benötigen. Sie sollten die Schlüsselrotation fortsetzen, damit Ihr Netzwerk vor Hackern vollständig geschützt ist.

Verwalten drahtloser Netzwerke

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie **Verfügbare drahtlose Netzwerke** aus, um drahtlose Netzwerke auszuwählen, zu denen Sie eine Verbindung herstellen oder an denen Sie sich anmelden möchten. Die Seite **Verfügbare drahtlose Netzwerke** wird angezeigt (Abbildung 2-2).

Abbildung 2-2. Die Seite "Verfügbare drahtlose Netzwerke"

Wenn Sie mit einem geschützten drahtlosen Netzwerk verbunden sind, werden die gesendeten und empfangenen Informationen verschlüsselt. Hacker können die im geschützten Netzwerk übertragenen Daten nicht abfangen und auch keine Verbindung zu Ihrem Netzwerk herstellen.

– Das Netzwerk ist geschützt.

– Das Netzwerk ist mithilfe von WEP- oder WPA-PSK-Sicherheit geschützt.

– Das Netzwerk ist ungeschützt; Sie können dennoch eine Verbindung dazu herstellen (nicht empfohlen).

Verbinden mit einem Netzwerk

Wählen Sie zum Herstellen einer Verbindung zu einem Netzwerk das gewünschte Netzwerk aus, und klicken Sie auf **Verbinden**. Wenn Sie für Ihren Router oder Zugriffspunkt einen vorinstallierten Schlüssel manuell konfiguriert haben, müssen Sie auch den Schlüssel eingeben.

Wenn das Netzwerk geschützt ist, müssen Sie sich anmelden, bevor Sie eine Verbindung mit dem Netzwerk herstellen können. Damit Sie sich anmelden können, muss Ihnen ein bereits mit dem Netzwerk verbundener Benutzer die Berechtigung dazu erteilen.

Wenn Sie sich an einem Netzwerk anmelden, können Sie die Verbindung mit dem Netzwerk erneut herstellen, ohne sich wieder anmelden zu müssen. Sie können auch anderen Benutzern die Berechtigung erteilen, sich an diesem Netzwerk anzumelden.

Trennen einer Netzwerkverbindung

Klicken Sie zum Trennen einer bestehenden Verbindung zu einem Netzwerk auf **Trennen**.

Verwenden erweiterter Optionen

Klicken Sie auf **Erweitert**, wenn Sie erweiterte Verbindungsoptionen verwenden möchten. Das Dialogfeld **Erweiterte Eigenschaften für drahtloses Netzwerk** wird angezeigt. In diesem Dialogfeld haben Sie die folgenden Möglichkeiten:

- Ändern der Reihenfolge der Netzwerke, zu denen automatisch eine Verbindung hergestellt wird – Das Netzwerk an erster Stelle in der Liste ist das Netzwerk, zu dem Sie zuletzt eine Verbindung hergestellt haben. Zu diesem Netzwerk versucht Wireless Home Network Security als Erstes, eine Verbindung herzustellen. Wählen Sie zum Verschieben eines Netzwerks das gewünschte Netzwerk aus, und klicken Sie auf **Nach oben** oder **Nach unten**. Wenn Sie zum Beispiel den Standort gewechselt haben und das Netzwerk, mit dem Sie zuletzt verbunden waren, weit entfernt ist und kein starkes Signal aufweist, können Sie ein Netzwerk mit einem stärkeren Signal an die erste Stelle der Liste setzen.
- Entfernen bevorzugter Netzwerke – Entfernen Sie Netzwerke aus dieser Liste. Wenn Sie beispielsweise versehentlich eine Verbindung zum Netzwerk Ihres Nachbarn hergestellt haben, wird es nun in der Liste aufgeführt. Wählen Sie das Netzwerk aus, und klicken Sie auf **Entfernen**, um es aus der Liste zu löschen.

- Ändern von Netzwerkeigenschaften – Wenn es beim Herstellen einer Verbindung zu einem ungeschützten Netzwerk zu Problemen kommt, können Sie dessen Eigenschaften ändern. Beachten Sie, dass diese Option nur für Netzwerke gilt, die nicht geschützt sind. Wählen Sie ein Netzwerk aus, und klicken Sie auf **Eigenschaften**, um dessen Eigenschaften zu ändern.
- Hinzufügen von Netzwerken ohne SSID-Übertragung – Wenn Sie beispielsweise eine Verbindung zum drahtlosen Netzwerk eines Freundes herstellen möchten, dieses aber nicht in der Liste aufgeführt wird, können Sie auf **Hinzufügen** klicken und die entsprechenden Informationen eingeben. Beachten Sie, dass das hinzugefügte Netzwerk nicht durch Wireless Home Network Security geschützt werden kann.

Konfigurieren von Optionen

Klicken Sie zum Konfigurieren von Optionen mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie dann **Optionen** aus. Die Seite **Optionen** wird angezeigt (Abbildung 2-3).

McAfee Wireless Home Network Security
McAfee
wirelesshomenetworksecurity
Hilfe
Zusammen-fassung
Verfügbare drahtlose Netzwerke
Optionen
Geschütztes drahtloses Netzwerk: angie
Einstellungen
Netzwerkereignisse anzeigen
Zeigt einen Bericht über Ereignisse in Ihrem Netzwerk an.
Erweiterte Einstellungen
Konfigurieren Sie erweiterte Einstellungen.
Extras
Zugriff widerrufen
Widerruft den Zugriff von Computern, die derzeit nicht verbunden sind.
Sicherheitsschlüssel manuell
Sicherheitsschlüssel des Netzwerks jetzt rotieren
Sicherheitseinstellungen
Repariert Sicherheitseinstellungen für Ihre drahtlosen Router und Zugriffspunkte.
Drahtlosen Router/Zugriffspunkt schützen
Fügen Sie eine drahtlosen Router oder Zugriffspunkt zu Ihrem geschützten Netzwerk hinzu.
Anderen Computer schützen
Erlaubt einem anderen Computer den Zugriff auf Ihr geschütztes Netzwerk.
Schutz für drahtlosen Router/Zugriffspunkt aufheben
Entfernen Sie eines drahtlosen Router oder Zugriffspunkt aus Ihrem geschützten Netzwerk.

Abbildung 2-3. Die Seite "Optionen"

Anzeigen von Ereignissen

Alle von Wireless Home Network Security durchgeführten Aktionen werden in Ereignisprotokollen vermerkt. Klicken Sie zum Anzeigen dieser Protokolle auf **Netzwerkereignisse anzeigen**. Die Informationen werden standardmäßig in chronologischer Reihenfolge angezeigt.

Im Feld **Ereignisse für das Netzwerk** können Sie auswählen, welche Art von Ereignissen angezeigt werden soll (unabhängig davon werden alle Ereignisse weiterhin protokolliert). Außerdem können Sie gegebenenfalls Ereignisse für jedes beliebige Netzwerk anzeigen, zu dem Sie gehören (falls Sie zu mehr als einem Netzwerk gehören).

Wenn ein Ereignis eintritt, wird eine Warnung mit einer kurzen Beschreibung angezeigt. Weitere Informationen zu Warnungen finden Sie unter *Grundlegendes zu Warnungen* auf Seite 30.

Konfigurieren erweiterter Einstellungen

Dieser Abschnitt richtet sich an erfahrene Benutzer. Klicken Sie auf **Erweiterte Einstellungen**, um Sicherheits-, Warnungs- und sonstige Einstellungen zu konfigurieren.

Nachdem Sie eine Einstellung geändert haben, klicken Sie auf **OK**, damit die Änderungen wirksam werden. Beachten Sie, dass nach dem Klicken auf **OK** bei allen verbundenen Computern die Verbindung vorübergehend (einige Minuten) getrennt wird.

Konfigurieren von Sicherheitseinstellungen

Verwenden Sie die Registerkarte **Sicherheitseinstellungen**, um Ihre Sicherheitseinstellungen zu ändern.

- Name des geschützten drahtlosen Netzwerks – Das ist der Name des derzeit geschützten Netzwerks. Wenn Sie den Namen eines Netzwerks ändern, wird es in der Liste **Verfügbare drahtlose Netzwerke** angezeigt, und Sie müssen dann eine neue Verbindung zu dem Netzwerk herstellen. Siehe *Verwalten drahtloser Netzwerke* auf Seite 21.

- Sicherheitsmodus – Das ist der aktuelle Sicherheitsmodus. Wenn Sie die Standardsicherheit (WEP) ändern möchten, wählen Sie WPA-PSK TKIP aus, um eine stärkere Verschlüsselung zu erhalten. Stellen Sie sicher, dass die Router, Zugriffspunkte und drahtlosen Adapter, die eine Verbindung zum Netzwerk herstellen, diesen Modus unterstützen. Andernfalls kann keine Verbindung hergestellt werden. Weitere Informationen zum Aktualisieren des Adapters finden Sie unter *Aktualisieren des drahtlosen Adapters* auf Seite 38.

- Automatische Schlüsselrotation aktivieren – Zum Aussetzen der Schlüsselrotation müssen Sie diese Option deaktivieren. Zum Ändern der Häufigkeit der Schlüsselrotation müssen Sie den Schieberegler verschieben. Weitere Informationen zur Schlüsselrotation finden Sie unter *Anzeigen Ihres geschützten drahtlosen Netzwerks* auf Seite 20.

- Benutzernamen oder Kennwort ändern – Sie können aus Sicherheitsgründen den standardmäßigen Benutzernamen oder das standardmäßige Kennwort für den drahtlosen Router oder Zugriffspunkt ändern, indem Sie ihn bzw. es auswählen und auf **Benutzernamen oder Kennwort ändern** klicken. Die Standardanmeldeinformationen haben Sie beim Anmelden und Konfigurieren Ihres Routers oder Zugriffspunktes angegeben.

Konfigurieren von Warnungseinstellungen

Verwenden Sie die Registerkarte **Warnungseinstellungen**, um Ihre Warnungseinstellungen zu ändern.

Wählen Sie die Art der Ereignisse aus, bei denen Sie gewarnt werden möchten, und klicken Sie auf **OK**. Wenn Sie auf bestimmte Arten von Ereignissen nicht aufmerksam gemacht werden möchten, müssen Sie die entsprechenden Kontrollkästchen deaktivieren.

Konfigurieren weiterer Einstellungen

Verwenden Sie die Registerkarte **Weitere Einstellungen**, um weitere Einstellungen zu ändern.

- Schlüssel in Klartext anzeigen – Für Netzwerke, die nicht durch Wireless Home Network Security geschützt sind. Schlüssel für ungeschützte Netzwerke, die in der Liste **Verfügbare drahtlose Netzwerke** aufgeführt sind, können in Klartext statt als Sternchen angezeigt werden. Wenn Sie Schlüssel in Klartext anzeigen, werden die Schlüssel aus Sicherheitsgründen verworfen.

- Alle gespeicherten Schlüssel verwerfen – Für Netzwerke, die nicht durch Wireless Home Network Security geschützt sind. Hierbei werden alle Schlüssel gelöscht, die gespeichert wurden. Hinweis: Wenn Sie diese Schlüssel löschen, müssen Sie erneut einen Schlüssel eingeben, wenn Sie eine Verbindung zu WEP- oder WPA-PSK-Netzwerken herstellen.

- Netzwerk verlassen – Für Netzwerke, die durch Wireless Home Network Security geschützt sind. Sie können Ihre Zugriffsrechte für ein geschütztes drahtloses Netzwerk aufgeben. Wenn Sie beispielsweise ein Netzwerk verlassen möchten und nicht vorhaben, später noch einmal eine Verbindung zu diesem Netzwerk herzustellen, können Sie es in der Liste auswählen und auf **Netzwerk verlassen** klicken.

- Bei einer Verbindung mit einem drahtlosen Netzwerk benachrichtigen – Beim Herstellen einer Verbindung wird eine Benachrichtigung angezeigt.

Widerrufen des Zugriffs auf das Netzwerk

So verhindern Sie, dass Computer auf das Netzwerk zugreifen, die angemeldet sind, aber derzeit keine Verbindung zum Netzwerk haben:

1. Klicken Sie auf **Zugriff widerrufen**. Das Dialogfeld **Zugriff widerrufen** wird angezeigt.
2. Klicken Sie auf **Widerrufen**.

Die Schlüsselrotation für das Netzwerk wird zurückgesetzt. Die aktuell verbundenen Computer erhalten den neuen Schlüssel und bleiben verbunden. Computer, die derzeit nicht verbunden sind, erhalten den aktualisierten Schlüssel nicht und müssen sich neu anmelden, bevor sie eine Verbindung herstellen können.

Wenn Sie den Zugriff für einen Computer widerrufen, kann der Computer erst nach erneuter Anmeldung wieder eine Verbindung zum geschützten Netzwerk herstellen. Dazu muss auf dem Computer Wireless Home Network Security installiert sein (siehe *Installieren von Wireless Home Network Security* auf Seite 17), und dann muss der Computer mit dem geschützten Netzwerk verbunden und dort angemeldet werden (siehe *Verbinden mit einem Netzwerk* auf Seite 22).

Reparieren von Sicherheitseinstellungen

Reparieren Sie die Sicherheitseinstellungen nur dann, wenn Sie Probleme mit Ihrem drahtlosen Netzwerk haben. Weitere Informationen finden Sie unter *Keine Verbindung möglich* auf Seite 38.

Gehen Sie zum Reparieren der Einstellungen für Router oder Zugriffspunkte im aktuellen Netzwerk folgendermaßen vor.

1. Klicken Sie auf **Sicherheitseinstellungen reparieren**. Das Dialogfeld **Reparieren** wird angezeigt.
2. Klicken Sie auf **Reparieren**.
3. Klicken Sie auf **Schließen**, wenn der Vorgang abgeschlossen ist.

Wenn keine Verbindung zu den Netzwerkroutern oder -zugriffspunkten hergestellt werden kann, wird eine Fehlermeldung angezeigt. Stellen Sie per Kabel eine Verbindung zu Ihrem Netzwerk her, und wiederholen Sie dann den Reparaturvorgang. Wenn das Kennwort für den Router oder Zugriffspunkt geändert wurde, werden Sie zur Eingabe des neuen Kennworts aufgefordert.

Schützen anderer Computer

Klicken Sie auf **Anderen Computer schützen**, um weitere Informationen zum Schützen anderer Computer und zum Gewähren von Zugriff auf das geschützte Netzwerk zu erhalten.

So schützen Sie einen anderen Computer:

1. Installieren Sie McAfee Wireless Home Network Security auf dem Computer, den Sie schützen möchten.
2. Klicken Sie auf dem Computer, den Sie schützen möchten, mit der rechten Maustaste auf das McAfee-Symbol ( ), zeigen Sie auf **Wireless Network Security**, und wählen Sie **Verfügbare drahtlose Netzwerke** aus. Die Seite **Verfügbare drahtlose Netzwerke** wird angezeigt.
3. Wählen Sie ein geschütztes Netzwerk aus, an dem Sie sich anmelden möchten, und klicken Sie auf **Verbinden**. Beachten Sie, dass Ihnen ein bereits mit dem Netzwerk verbundener Benutzer die Berechtigung zum Anmelden erteilen muss.

   Wenn Sie sich an einem Netzwerk anmelden, können Sie die Verbindung mit dem Netzwerk erneut herstellen, ohne sich wieder anmelden zu müssen. Sie können auch anderen Benutzern die Berechtigung erteilen, sich an diesem Netzwerk anzumelden.
4. Klicken Sie im Bestätigungsdialogfeld auf **OK**.

Wenn Sie drahtlose Geräte, die von Wireless Home Network Security nicht unterstützt werden, mit dem Netzwerk verbinden (z. B. einen Handheld), gehen Sie folgendermaßen vor.

1. Klicken Sie zum Anzeigen dieser Protokolle auf **Netzwerkereignisse anzeigen**.
2. Notieren Sie den Schlüssel.
3. Klicken Sie auf **Schlüsselrotation aussetzen**. Durch Aussetzen der Schlüsselrotation wird verhindert, dass die Verbindung zu manuell mit dem Netzwerk verbundenen Geräten getrennt wird.
4. Geben Sie den Schlüssel im Gerät ein.

Klicken Sie auf **Schlüsselrotation fortsetzen**, wenn Sie diese Geräte nicht mehr benötigen. Sie sollten die Schlüsselrotation fortsetzen, damit Ihr Netzwerk vor Hackern vollständig geschützt ist.

Rotieren des Schlüssels

Klicken Sie auf **Sicherheitsschlüssel manuell rotieren**, um den Sicherheitsschlüssel für das Netzwerk zu rotieren.

Schützen drahtloser Netzwerke

Gehen Sie zum Schützen eines Routers oder Zugriffspunktes folgendermaßen vor.

1. Klicken Sie auf **Drahtlosen Router/Zugriffspunkt schützen**. Das Dialogfeld **Drahtloses Netzwerk schützen** wird angezeigt. Wenn der Router oder Zugriffspunkt nicht in der Liste aufgeführt wird, klicken Sie auf **Aktualisieren**.
2. Wählen Sie den zu schützenden Router oder Zugriffspunkt aus, und klicken Sie auf **Schützen**.

Aufheben des Schutzes drahtloser Netzwerke

Sie müssen mit dem drahtlosen Router oder Zugriffspunkt verbunden sein, dessen Schutz Sie aufheben möchten.

Gehen Sie zum Aufheben des Schutzes eines Routers oder Zugriffspunktes folgendermaßen vor.

1. Klicken Sie auf **Schutz für drahtlosen Router/Zugriffspunkt aufheben**. Das Dialogfeld **Schutz für drahtloses Netzwerk aufheben** wird angezeigt. Wenn der Router oder Zugriffspunkt nicht in der Liste aufgeführt wird, klicken Sie auf **Aktualisieren**.
2. Wählen Sie den Router oder Zugriffspunkt aus, dessen Schutz Sie aufheben möchten, und klicken Sie auf **Schutz aufheben**.

Aktualisieren von Wireless Home Network Security

Wenn Sie mit dem Internet verbunden sind, prüft Wireless Home Network Security alle vier Stunden, ob Software-Updates zur Verfügung stehen, lädt diese dann automatisch herunter und installiert wöchentliche Updates, ohne Sie bei der Arbeit zu unterbrechen. Das Herunterladen dieser Updates beeinträchtigt die Leistung Ihres Systems nur minimal.

Bei einem Produktupdate erhalten Sie eine entsprechende Benachrichtigung. Sie können dann entscheiden, ob Wireless Home Network Security aktualisiert werden soll.

Automatisches Prüfen auf Updates

McAfee SecurityCenter ist so konfiguriert, dass es bei bestehender Internetverbindung alle vier Stunden automatisch nach Updates für Ihre McAfee-Dienste sucht und Sie dann durch entsprechende Meldungen und akustische Signale benachrichtigt. Standardmäßig werden verfügbare Updates automatisch von SecurityCenter heruntergeladen und installiert.

HINWEIS
In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie alle Programme, bevor Sie den Neustart durchführen.

Manuelles Prüfen auf Updates

Zusätzlich zur automatischen Suche nach Updates, die bei einer bestehenden Internetverbindung durchgeführt wird, können Sie auch jederzeit manuell nach Updates suchen.

So prüfen Sie manuell, ob Updates für Wireless Home Network Security verfügbar sind:

1. Stellen Sie sicher, dass Ihr Computer mit dem Internet verbunden ist.
2. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, und klicken Sie dann auf **Aktualisieren**. Das Dialogfeld **SecurityCenter-Updates** wird angezeigt.
3. Klicken Sie auf **Jetzt prüfen**.

   Wenn ein Update vorhanden ist, wird das Dialogfeld **McAfee SecurityCenter** angezeigt. Klicken Sie auf **Aktualisieren**, um den Vorgang fortzusetzen.

   Wenn keine Updates verfügbar sind, werden Sie in einem Dialogfeld darüber informiert, dass Wireless Home Network Security auf dem neuesten Stand ist. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.
4. Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden. Das Update wird automatisch vom **Update-Assistenten** installiert.
5. Klicken Sie nach Abschluss der Update-Installation auf **Fertig stellen**.

   HINWEIS
   In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Speichern Sie Ihre Arbeit, und schließen Sie alle Programme, bevor Sie den Neustart durchführen.

Grundlegendes zu Warnungen

Warnungen werden bei bestimmten Ereignissen angezeigt. Sie informieren Sie über Änderungen im Netzwerk.

Computer gesichert

Ein Benutzer, der Zugriff auf das geschützte Netzwerk besitzt, hat einem anderen Benutzer Zugriff gewährt. Beispiel: Der Benutzer "Lance" hat dem Benutzer "Mercks" Zugriff gewährt. Beide können nun das drahtlose Netzwerk "CoppiWAP" nutzen.

Computer getrennt

Ein Benutzer hat die Netzwerkverbindung getrennt. Weitere Informationen finden Sie unter *Trennen einer Netzwerkverbindung* auf Seite 22.

Computer verbunden

Ein Benutzer hat eine Verbindung zum Netzwerk hergestellt. Weitere Informationen finden Sie unter *Verbinden mit einem Netzwerk* auf Seite 22.

Drahtloser Router/Zugriffspunkt geschützt

Ein drahtloser Router oder Zugriffspunkt wurde in Ihrem Netzwerk geschützt. Weitere Informationen finden Sie unter *Schützen drahtloser Netzwerke* auf Seite 28.

Fehler bei der Schlüsselrotation

Fehlerursache:

- Die Anmeldeinformationen für Ihren Router oder Zugriffspunkt wurden geändert. Wenn Sie wissen, wie die Anmeldeinformationen lauten, finden Sie weitere Informationen unter *Reparieren von Sicherheitseinstellungen* auf Seite 26.
- Die Firmware-Version Ihres Routers oder Zugriffspunktes wurde geändert, und die neue Version wird nicht unterstützt. Weitere Informationen finden Sie unter *Keine Verbindung möglich* auf Seite 38.
- Ihr Router oder Zugriffspunkt ist nicht verfügbar. Stellen Sie sicher, dass der Router oder Zugriffspunkt eingeschaltet und an das Netzwerk angeschlossen ist.
- Fehler durch doppelte Administratoren. Weitere Informationen finden Sie unter *Fehler durch doppelte Administratoren* auf Seite 35.

Bei Problemen mit dem Herstellen einer Verbindung zum Netzwerk finden Sie weitere Informationen unter *Reparieren von Sicherheitseinstellungen* auf Seite 26.

Häufigkeit der Sicherheitsschlüsselrotation geändert

Der Häufigkeit der Sicherheitsschlüsselrotation für das Netzwerk wurde geändert. McAfee Wireless Home Network Security ändert automatisch den Verschlüsselungsschlüssel für das Netzwerk. Das erschwert Hackern, Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk herzustellen.

Kennwort geändert

Ein Benutzer hat den Benutzernamen oder das Kennwort für einen Router oder Zugriffspunkt im Netzwerk geändert. Weitere Informationen finden Sie unter *Konfigurieren von Sicherheitseinstellungen* auf Seite 24.

Netzwerk repariert

Ein Benutzer hat aufgrund von Problemen beim Herstellen einer Verbindung versucht, das Netzwerk zu reparieren.

Netzwerk umbenannt

Ein Benutzer hat das Netzwerk umbenannt. Sie müssen die Verbindung mit dem Netzwerk neu herstellen. Weitere Informationen finden Sie unter *Verbinden mit einem Netzwerk* auf Seite 22.

Netzwerkeinstellungen geändert

Ein Benutzer ist im Begriff, die Sicherheitseinstellungen des Netzwerks zu ändern. Unter Umständen wird während dieses Vorgangs die Verbindung kurz unterbrochen. Mindestens eine der folgenden Einstellungen wird geändert:

- Name des Netzwerks
- Sicherheitsmodus
- Häufigkeit der Schlüsselrotation
- Status der automatischen Schlüsselrotation

Netzwerkkonfiguration geändert

Ein Benutzer hat den Sicherheitsmodus für das Netzwerk geändert. Weitere Informationen finden Sie unter *Konfigurieren von Sicherheitseinstellungen* auf Seite 24.

Schlüsselrotation ausgesetzt

Ein Benutzer hat die Schlüsselrotation ausgesetzt. Sie sollten die Schlüsselrotation fortsetzen, damit Ihr Netzwerk vollständig vor Hackern geschützt ist.

Schlüsselrotation fortgesetzt

Ein Benutzer hat die Schlüsselrotation fortgesetzt. Durch die Schlüsselrotation wird verhindert, dass Hacker auf das Netzwerk zugreifen.

Schutz für drahtlosen Router/Zugriffspunkt aufgehoben

Ein drahtloser Router oder Zugriffspunkt wurde aus dem Netzwerk entfernt. Weitere Informationen finden Sie unter *Aufheben des Schutzes drahtloser Netzwerke* auf Seite 28.

Sicherheitsschlüssel rotiert

Der Sicherheitsschlüssel für das Netzwerk wurde geändert. McAfee Wireless Home Network Security ändert automatisch den Verschlüsselungsschlüssel für das Netzwerk. Das erschwert Hackern, Daten abzufangen oder eine Verbindung zu Ihrem Netzwerk herzustellen.

Zugriff widerrufen

Ein Benutzer hat den Netzwerkschlüssel aktualisiert. Weitere Informationen finden Sie unter *Widerrufen des Zugriffs auf das Netzwerk* auf Seite 26.

Problembehandlung

In diesem Abschnitt werden Verfahren zur Problembehandlung für McAfee Wireless Home Network Security und Hardware von Drittanbietern beschrieben.

Installation

In diesem Abschnitt wird erklärt, wie Installationsprobleme behoben werden.

Auf welchen Computern muss diese Software installiert werden?

Installieren Sie McAfee Wireless Home Network Security auf allen drahtlosen Computern im Netzwerk (im Gegensatz zu anderen McAfee-Anwendungen können Sie diese Software auf mehreren Computern installieren).

Auf Computern ohne drahtlosen Adapter können Sie die Software installieren (müssen dies aber nicht tun). Auf diesen Computern ist die Software nicht aktiv, weil sie keinen entsprechenden Schutz benötigen. Den Router oder Zugriffspunkt müssen Sie von einem der drahtlosen Computer aus schützen (siehe *Schützen drahtloser Netzwerke* auf Seite 28), um das Netzwerk zu sichern.

Drahtloser Adapter wird nicht erkannt

Wenn der drahtlose Adapter nach dem Installieren und Aktivieren nicht erkannt wird, müssen Sie den Computer neu starten. Wird der Adapter anschließend immer noch nicht erkannt, sollten Sie folgendermaßen vorgehen:

1. Öffnen Sie das Dialogfeld **Eigenschaften von Drahtlose Netzwerkverbindung**.
2. Deaktivieren Sie das Kontrollkästchen **MWL-Filter**, und aktivieren Sie es anschließend wieder.
3. Klicken Sie auf **OK**.

Wenn das nicht funktioniert, wird der drahtlose Adapter möglicherweise nicht unterstützt. Aktualisieren Sie den Adapter, oder erwerben Sie einen neuen. Eine Liste der unterstützten Adapter finden Sie unter http://www.mcafee.com/de/router. Informationen zum Aktualisieren des Adapters finden Sie unter *Aktualisieren des drahtlosen Adapters* auf Seite 38.

Mehrere drahtlose Adapter

Wenn in einer Fehlermeldung steht, dass mehrere drahtlose Adapter installiert sind, müssen Sie alle bis auf einen deaktivieren oder vom Netzwerk trennen. Wireless Home Network Security funktioniert nur mit einem drahtlosen Adapter.

Kein Download auf drahtlose Computer möglich, da das Netzwerk bereits sicher ist

Installieren Sie, falls Sie über eine CD verfügen, McAfee Wireless Home Network Security von der CD auf allen drahtlosen Computern.

Wenn Sie die Software auf einem drahtlosen Computer installiert und das Netzwerk geschützt haben, bevor Sie die Software auf allen anderen Computern installiert haben, verfügen Sie über folgende Optionen.

- Heben Sie den Schutz des Netzwerks auf (siehe *Aufheben des Schutzes drahtloser Netzwerke* auf Seite 28). Laden Sie dann die Software herunter, und installieren Sie sie auf allen drahtlosen Computern. Schützen Sie Ihr Netzwerk dann wieder (siehe *Schützen drahtloser Netzwerke* auf Seite 28).
- Zeigen Sie den Netzwerkschlüssel an (siehe *Anzeigen Ihres geschützten drahtlosen Netzwerks* auf Seite 20). Geben Sie dann den Schlüssel auf Ihrem drahtlosen Computer ein, um eine Verbindung zum Netzwerk herzustellen. Laden Sie die Software herunter, installieren Sie sie, und melden Sie sich vom drahtlosen Computer aus am Netzwerk an (siehe *Schützen anderer Computer* auf Seite 27).
- Laden Sie die ausführbare Datei auf den Computer herunter, der bereits mit dem Netzwerk verbunden ist, und speichern Sie sie auf einem USB-Speicherstick, oder brennen Sie sie auf eine CD, damit Sie sie auf den anderen Computern installieren können.

Schützen oder Konfigurieren des Netzwerks

In diesem Abschnitt wird die Behandlung von Problemen erläutert, die beim Schützen oder Konfigurieren eines Netzwerkes auftreten.

Nicht unterstützter Router oder Zugriffspunkt

Wenn es in einer Fehlermeldung heißt, dass der drahtlose Router oder Zugriffspunkt unter Umständen nicht unterstützt wird, konnte das Gerät von McAfee Wireless Home Network Security nicht konfiguriert werden, weil es nicht erkannt oder gefunden wurde.

Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Home Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Router und Zugriffspunkte aus). Wenn der Router oder Zugriffspunkt in der Liste unter http://www.mcafee.com/de/router aufgeführt wird und dieser Fehler dennoch auftritt, liegen Kommunikationsprobleme zwischen Ihrem Computer und dem Router oder Zugriffspunkt vor. Lesen Sie *Keine Verbindung möglich* auf Seite 38, bevor Sie das Netzwerk wieder schützen.

Aktualisieren der Firmware des Routers oder Zugriffspunktes

Wenn es in einer Fehlermeldung heißt, dass die Firmware-Version des drahtlosen Routers oder Zugriffspunktes nicht unterstützt wird, wird zwar das Gerät unterstützt, nicht aber dessen Firmware-Version. Stellen Sie durch Anforderung eines Updates sicher, dass Sie über die neueste Version von Wireless Home Network Security verfügen (McAfee weitet die Unterstützung ständig auf neue Firmware-Versionen aus).

Wenn Sie über die neueste Version von Wireless Home Network Security verfügen, sollten Sie die Website des Herstellers des Routers oder Zugriffspunktes aufrufen bzw. sich an dessen Support wenden und eine unter http://www.mcafee.com/de/router aufgelistete Firmware-Version installieren.

Fehler durch doppelte Administratoren

Nach dem Konfigurieren des Routers oder Zugriffspunktes müssen Sie sich von der Administrationsoberfläche abmelden. Geschieht das nicht, verhält der Router oder Zugriffspunkt sich in einigen Fällen so, als würde er weiterhin von einem anderen Computer konfiguriert werden. Es wird dann eine Fehlermeldung angezeigt.

Wenn Sie sich nicht abmelden können, ziehen Sie das Stromkabel Ihres Routers oder Zugriffspunktes heraus, und stecken Sie es dann wieder ein.

Netzwerk als ungesichert angezeigt

Wenn das Netzwerk als ungesichert angezeigt wird, ist es nicht geschützt. Sie müssen das Netzwerk schützen (siehe *Schützen drahtloser Netzwerke* auf Seite 28), um es zu sichern. Beachten Sie, dass McAfee Wireless Home Network Security nur mit kompatiblen Routern und Zugriffspunkten funktioniert (siehe http://www.mcafee.com/de/router).

Keine Reparatur möglich

Gehen Sie folgendermaßen vor, wenn bei der Reparatur Fehler auftreten. Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Stellen Sie per Kabel eine Verbindung zu Ihrem Netzwerk her, und wiederholen Sie dann den Reparaturvorgang.
- Ziehen Sie das Stromkabel des Routers oder Zugriffspunktes, und stecken Sie es dann wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und reparieren Sie ihn.
- Verlassen Sie mithilfe der erweiterten Optionen das Netzwerk auf allen Computern, setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie ihn dann.

Verbinden von Computern mit Ihrem Netzwerk

In diesem Abschnitt wird die Behandlung von Problemen erläutert, die beim Verbinden von Computern zum Netzwerk auftreten.

Warten auf Autorisierung

Wenn Sie sich an einem geschützten Netzwerk anzumelden versuchen und der Computer vergeblich auf Autorisierung wartet, sollten Sie Folgendes überprüfen.

- Ein drahtloser Computer mit bestehendem Zugriff auf das Netzwerk ist eingeschaltet und mit dem Netzwerk verbunden.
- An diesem Computer ist jemand anwesend, der Zugriff erteilen kann, wenn Ihr Computer angezeigt wird.
- Die Computer befinden sich innerhalb der Reichweite der Funkwellen.

Wenn **Zugriff gewähren** auf dem Computer mit bestehendem Zugriff auf das Netzwerk nicht angezeigt wird, müssen Sie versuchen, den Zugriff von einem anderen Computer aus zu gewähren.

Falls keine anderen Computer verfügbar sind, müssen Sie den Schutz des Netzwerks vom Computer mit vorhandenem Zugriff aus aufheben und das Netzwerk vom Computer ohne Zugriff aus schützen. Melden Sie sich anschließend von dem Computer aus am Netzwerk an, der das Netzwerk ursprünglich schützte.

Gewähren von Zugriff für einen unbekannten Computer

Wenn Sie von einem unbekannten Computer eine Anforderung zum Gewähren von Zugriff erhalten, sollten Sie überprüfen, woher sie stammt. Möglicherweise versucht ein Unbefugter, auf Ihr Netzwerk zuzugreifen.

Verbinden mit einem Netzwerk oder dem Internet

In diesem Abschnitt wird die Behandlung von Problemen beim Herstellen einer Verbindung zu einem Netzwerk oder dem Internet erläutert.

Schlechte Verbindung zum Internet

Wenn Sie keine Verbindung herstellen können, schließen Sie den Computer mit einem Kabel an das Netzwerk an, und stellen Sie dann eine Verbindung zum Internet her. Ist immer noch keine Verbindung möglich, sollten Sie die folgenden Punkte überprüfen:

- Ihr Modem ist eingeschaltet.
- Ihre PPPoE-Einstellungen (siehe *Glossar* auf Seite 42) sind korrekt.
- Ihre DSL- oder Kabelleitung ist aktiv.

Verbindungsprobleme, etwa mit der Geschwindigkeit und der Signalstärke, können auch durch Funkstörungen verursacht werden. Wechseln Sie den Kanal Ihres schnurlosen Telefons, beseitigen Sie mögliche Störquellen, oder stellen Sie Ihren drahtlosen Router, Zugriffspunkt oder Computer an einem anderen Ort auf.

Kurze Unterbrechung der Verbindung

Wenn Ihre Verbindung kurz unterbrochen wird (z. B. während eines Online-Spiels), kann das daran liegen, dass die Schlüsselrotation kurze Verzögerungen im Netzwerk verursacht: Setzen Sie die Schlüsselrotation vorübergehend aus. Sie sollten die Schlüsselrotation möglichst bald fortsetzen, damit das Netzwerk vor Hackern vollständig geschützt ist.

Verbindungsverlust bei Geräten (nicht beim Computer)

Wenn beim Einsatz von McAfee Wireless Home Network Security einige Geräte die Verbindung verlieren, setzen Sie die Schlüsselrotation aus.

Aufforderung zur Eingabe des WEP- oder WPA-Schlüssels

Wenn Sie zum Herstellen einer Verbindung zum Netzwerk einen WEP- oder WPA-Schlüssel eingeben müssen, haben Sie wahrscheinlich die Software nicht auf Ihrem Computer installiert. Für eine ordnungsgemäße Funktionsweise muss Wireless Home Network Security auf allen drahtlosen Computern im Netzwerk installiert sein. Siehe *Schützen oder Konfigurieren des Netzwerks* auf Seite 34.

Keine Verbindung möglich

Wenn Sie keine Verbindung herstellen können, gehen Sie folgendermaßen vor: Beachten Sie, dass die einzelnen Verfahren voneinander unabhängig sind.

- Vergewissern Sie sich, falls Sie keine Verbindung zu einem geschützten Netzwerk herstellen, dass Sie über den richtigen Schlüssel verfügen. Geben Sie ihn erneut ein.
- Ziehen Sie den Stecker des drahtlosen Adapters, und stecken Sie ihn wieder ein. Oder deaktivieren Sie den Adapter, und aktivieren Sie ihn dann wieder.
- Schalten Sie den Router oder Zugriffspunkt aus und wieder ein. Versuchen Sie dann, eine Verbindung herzustellen.
- Vergewissern Sie sich, dass der drahtlose Router oder Zugriffspunkt verbunden ist, und reparieren Sie die Sicherheitseinstellungen (siehe *Reparieren von Sicherheitseinstellungen* auf Seite 26).

  Wenn bei der Reparatur Fehler auftreten, finden Sie weitere Informationen unter *Keine Reparatur möglich* auf Seite 35.
- Starten Sie den Computer neu.
- Aktualisieren Sie den drahtlosen Adapter, oder erwerben Sie einen neuen. Informationen zum Aktualisieren des Adapters finden Sie unter *Aktualisieren des drahtlosen Adapters* auf Seite 38. Beispiel: Im Netzwerk kommt WPA-PSK TKIP-Sicherheit zum Einsatz, und der drahtlose Adapter unterstützt den Sicherheitsmodus des Netzwerks nicht (das Netzwerk zeigt WEP an, obwohl es auf WPA eingestellt ist).
- Wenn Sie nach dem Aktualisieren des drahtlosen Routers oder Zugriffspunktes keine Verbindung herstellen können, haben Sie möglicherweise auf eine nicht unterstützte Version aktualisiert. Vergewissern Sie sich, dass der Router oder Zugriffspunkt unterstützt wird. Wenn dies nicht der Fall ist, sollten Sie eine unterstützte Version installieren oder warten, bis ein Update von Wireless Home Network Security verfügbar ist.

Aktualisieren des drahtlosen Adapters

Gehen Sie zum Aktualisieren Ihres Adapters folgendermaßen vor:

1. Klicken Sie auf dem Desktop auf **Start**, zeigen Sie auf **Einstellungen**, und wählen Sie dann **Systemsteuerung** aus.
2. Doppelklicken Sie auf das Symbol **System**. Das Dialogfeld **Systemeigenschaften** wird angezeigt.
3. Wählen Sie die Registerkarte **Hardware** aus, und klicken Sie dann auf **Geräte-Manager**.
4. Doppelklicken Sie in der Liste **Geräte-Manager** auf den Adapter.

5 Wählen Sie die Registerkarte **Treiber** aus, und notieren Sie sich den Treiber, der bei Ihnen installiert ist.

6 Gehen Sie zur Website des Adapterherstellers, und überprüfen Sie, ob ein Update verfügbar ist. Treiber sind meist im Support- oder Download-Bereich zu finden.

7 Wenn ein Treiber-Update verfügbar ist, folgen Sie den Anweisungen auf der Website, um das Update herunterzuladen.

8 Gehen Sie zurück zur Registerkarte **Treiber**, und klicken Sie auf **Aktualisieren**. Ein Windows-Assistent wird angezeigt.

9 Folgen Sie den Anweisungen auf dem Bildschirm.

Schwaches Signal

Wenn Ihre Verbindung unterbrochen wird oder sehr langsam ist, ist möglicherweise das Signal zu schwach. Gehen Sie wie folgt vor, um das Signal zu verbessern.

- Stellen Sie sicher, dass die drahtlosen Geräte nicht durch Metallobjekte wie Öfen, Rohre oder große Haushaltsgeräte blockiert werden. Funksignale werden stark abgeschwächt, wenn sie durch solche Objekte hindurch verlaufen.
- Wenn das Signal durch Wände gelangen muss, sollten Sie sicherstellen, dass dies nicht im spitzen Winkel geschieht. Je länger der Weg innerhalb der Wand ist, desto schwächer wird das Signal.
- Verfügt der drahtlose Router oder Zugriffspunkt über zwei Antennen, sollten Sie die beiden Antennen nach Möglichkeit rechtwinklig zueinander ausrichten (eine vertikal und eine horizontal im 90-Grad-Winkel).
- Einige Hersteller verwenden Hochleistungsantennen. Richtantennen haben eine größere Reichweite, während omnidirektionale Antennen (Rundstrahler) die größte Flexibilität bieten. Richten Sie sich beim Installieren der Antenne nach den entsprechenden Anweisungen des Herstellers.

Führen diese Schritte nicht zum Erfolg, sollten Sie dem Netzwerk einen Zugriffspunkt hinzufügen, der sich näher an dem Computer befindet, zu dem Sie eine Verbindung herstellen möchten. Wenn Sie den zweiten Zugriffspunkt mit demselben Netzwerknamen (SSID) und einem anderen Kanal konfigurieren, sucht der Adapter automatisch das stärkste Signal und stellt die Verbindung über den entsprechenden Zugriffspunkt her.

Windows kann die drahtlose Verbindung nicht konfigurieren

Wenn Sie eine Meldung erhalten, dass Windows die drahtlose Verbindung nicht konfigurieren kann, können Sie sie ignorieren. Verwenden Sie Wireless Home Network Security, um Verbindungen zu drahtlosen Netzwerken herzustellen und die Netzwerke zu konfigurieren. Stellen Sie sicher, dass im Windows-Dialogfeld **Eigenschaften von Drahtlose Netzwerkverbindung** auf der Registerkarte **Drahtlosnetzwerke** das Kontrollkästchen **Windows zum Konfigurieren der Einstellungen verwenden** deaktiviert ist.

Windows zeigt keine Verbindung an

Wenn Sie verbunden sind, das Netzwerksymbol von Windows jedoch ein X anzeigt (d. h. keine Verbindung), so können Sie das ignorieren. Ihre Verbindung ist einwandfrei.

Andere Probleme

In diesem Abschnitt wird die Behandlung sonstiger Probleme erläutert.

Bei Verwendung anderer Programme lautet der Netzwerkname anders

Dass der Name des Netzwerks in anderen Programmen anders angezeigt wird (etwa mit _SafeAaf als Bestandteil des Namens), ist völlig normal. Wireless Home Network Security kennzeichnet Netzwerke mit einem Code, wenn sie geschützt sind.

Probleme beim Konfigurieren drahtloser Router oder Zugriffspunkte

Wenn beim Konfigurieren des Routers oder Zugriffspunktes oder beim Hinzufügen mehrerer Router im Netzwerk ein Fehler auftritt, müssen Sie sich vergewissern, dass alle Router und Zugriffspunkte über eine eigene IP-Adresse verfügen.

Wenn der Name des drahtlosen Routers oder Zugriffspunktes im Dialogfeld **Drahtlosen Router/Zugriffspunkt schützen** aufgeführt wird, Sie jedoch bei dessen Konfiguration eine Fehlermeldung erhalten, müssen Sie überprüfen, ob der Router oder Zugriffspunkt unterstützt wird. Eine Liste der unterstützten Router und Zugriffspunkte finden Sie unter http://www.mcafee.com/de/router.

Wenn der Router oder Zugriffspunkt konfiguriert ist, sich aber scheinbar nicht im richtigen Netzwerk befindet (es werden zum Beispiel keine anderen Computer im LAN angezeigt), müssen Sie sicherstellen, dass Sie den richtigen Router oder Zugriffspunkt konfiguriert haben, und nicht den Ihres Nachbarn. Ziehen Sie das Stromkabel des Routers oder Zugriffspunktes, und vergewissern Sie sich, dass die Verbindung unterbrochen wird. Wenn Sie den falschen Router oder Zugriffspunkt konfiguriert haben, heben Sie dessen Schutz wieder auf, und schützen Sie dann den richtigen Router oder Zugriffspunkt.

Wenn Sie den Router oder Zugriffspunkt nicht ordnungsgemäß konfigurieren oder hinzufügen können, er aber unterstützt wird, liegt das unter Umständen daran, dass Sie Änderungen durchgeführt haben, die nun eine ordnungsgemäße Konfiguration verhindern.

- Folgen Sie den Anweisungen des Herstellers zum Konfigurieren Ihres drahtlosen Routers bzw. Zugriffspunktes für DHCP oder zum Festlegen der richtigen IP-Adresse. In einigen Fällen ist ein Konfigurations-Tool im Lieferumfang des Produkts enthalten.
- Setzen Sie den Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und versuchen Sie erneut, das Netzwerk zu reparieren. Möglicherweise haben Sie den Administrationsport am Router oder Zugriffspunkt geändert oder die drahtlose Administration deaktiviert. Stellen Sie sicher, dass Sie die Standardkonfiguration verwenden und dass die drahtlose Konfiguration aktiviert ist. Eine weitere Möglichkeit besteht darin, dass die http-Administration deaktiviert ist. Stellen Sie in diesem Fall sicher, dass sie aktiviert ist.
- Wenn der drahtlose Router oder Zugriffspunkt nicht in der Liste drahtloser Router oder Zugriffspunkte aufgeführt wird, die geschützt und zu denen Verbindungen hergestellt werden sollen, müssen Sie die SSID-Übertragung aktivieren und sicherstellen, dass der Router oder Zugriffspunkt aktiviert ist.
- Falls Sie getrennt werden oder keine Verbindung herstellen können, ist möglicherweise die MAC-Filterung aktiviert. Deaktivieren Sie sie.
- Wenn zwischen zwei Computern mit drahtloser Verbindung zum Netzwerk keine Netzwerkvorgänge möglich sind (zum Beispiel die Freigabe von Dateien oder das Drucken auf freigegebenen Druckern), müssen Sie überprüfen, ob die Isolierung von Zugriffspunkten nicht aktiviert ist. Sie verhindert, dass drahtlose Computer über das Netzwerk miteinander in Verbindung treten können.

Ersetzen von Computern

Wenn der Computer, der das Netzwerk geschützt hat, ersetzt wurde ist und es keine anderen Computer mit Zugriff gibt (d. h. Sie können nicht auf das Netzwerk zugreifen), setzen Sie den drahtlosen Router oder Zugriffspunkt auf die Werkseinstellungen zurück, und schützen Sie das Netzwerk erneut.

Software funktioniert nach dem Aktualisieren des Betriebssystems nicht

Wenn Wireless Home Network Security nach dem Aktualisieren von Betriebssystemen nicht mehr funktioniert, müssen Sie es deinstallieren und dann neu installieren.

Glossar

802.11

Eine Reihe von IEEE-Standards für Funk-LANs. 802.11 legt eine Schnittstelle für den Funkverkehr zwischen einem drahtlosen Client und einer Basisstation oder zwischen zwei drahtlosen Clients fest. Zu den verschiedenen Spezifikationen von 802.11 gehören die Standards 802.11a (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band), 802.11b (für Netzwerke mit einer Bandbreite bis zu 11 Mbit/s im 2,4 GHz-Band), 802.11g (für Netzwerke mit einer Bandbreite bis zu 54 Mbit/s im 2,4 GHz-Band) sowie und 802.11i (eine Reihe von Sicherheitsstandards für alle drahtlosen Ethernet-Netzwerke).

802.11a

Eine Erweiterung von 802.11 für Funk-LANs zum Senden von Daten mit einer Bandbreite bis zu 54 Mbit/s im 5 GHz-Band. Dabei ist die Übertragungsgeschwindigkeit zwar größer als bei 802.11b, die Reichweite ist jedoch viel geringer.

802.11b

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 11 Mbit/s im 2,4 GHz-Band bietet. 802.11b gilt derzeit als Standard für drahtlose Netzwerkverbindungen.

802.11g

Eine Erweiterung von 802.11 für Funk-LANs, die eine Bandbreite von 54 Mbit/s im 2,4 GHz-Band bietet.

802.1x

Wird von Wireless Home Network Security nicht unterstützt. Ein IEEE-Standard für die Authentifizierung in kabelgebundenen und drahtlosen Netzwerken, wird aber vor allem in Verbindung mit drahtlosen 802.11-Netzwerken verwendet. Dieser Standard bietet eine starke gegenseitige Authentifizierung zwischen einem Client und einem Authentifizierungsserver. Außerdem bietet 802.1x dynamische, benutzer- und sitzungsspezifische WEP-Schlüssel, wodurch der bei statischen WEP-Schlüsseln übliche Verwaltungsaufwand und die Sicherheitsrisiken beseitigt werden.

A

Authentifizierung

Der Vorgang des Identifizierens eines bestimmten Benutzers, meist anhand von Benutzername und Kennwort. Mit der Authentifizierung wird sichergestellt, dass es sich bei einem Benutzer auch wirklich um denjenigen handelt, der er oder sie zu sein vorgibt. Über die Zugriffsrechte dieses Benutzers sagt die Authentifizierung jedoch nichts aus.

B

Bandbreite

Die Datenmenge, die innerhalb eines bestimmten Zeitraums übertragen werden kann. Bei digitalen Geräten wird die Bandbreite meist in Bit pro Sekunde (Bit/s) oder Byte pro Sekunde angegeben. Bei analogen Geräten wird die Bandbreite als Taktzahl pro Sekunde bzw. Hertz (Hz) angegeben.

Brute-Force-Angriff

Eine Vorgehensweise nach dem Fehler-Treffer-Prinzip, die auch unter dem Begriff "Brute-Force-Cracking" bekannt ist. Dabei versuchen entsprechende Programme, verschlüsselte Daten (z. B. Kennwörter) mithilfe eines riesigen Aufwands (mit "purer Gewalt") anstatt durch zielgerichtete Strategien zu entschlüsseln. Brute-Force-Anwendungen probieren nacheinander alle möglichen Kombinationen von zulässigen Zeichen aus – wie bei einem Safe, bei dem alle Zahlenkombinationen ausprobiert werden, um ihn zu öffnen, was genauso eine strafbare Handlung ist. Brute-Force-Angriffe werden als eine Methode betrachtet, die, wenn auch mit großen Zeitaufwand verbunden, irgendwann schließlich zum Erfolg führt.

C

Chiffrierter Text

Das sind Daten, die verschlüsselt wurden. Chiffrierter Text ist nicht lesbar, solange er nicht mithilfe eines Schlüssels wieder in Klartext umgewandelt (entschlüsselt) wurde.

Client

Eine Anwendung, die auf einem PC oder einer Workstation ausgeführt wird und zum Durchführen bestimmter Vorgänge auf einen Server angewiesen ist. Beispiel: Ein E-Mail-Client ist eine Anwendung, mit der Sie E-Mails senden und empfangen können.

D

Denial of Service, DoS

Ein DoS-Angriff (Denial-of-Service, Dienstverweigerung) ist ein Störfall im Internet, durch den Benutzer oder Unternehmen nicht mehr auf bestimmte Ressourcen oder Dienste zugreifen können. Dabei handelt es sich meist um die Nichtverfügbarkeit eines einzelnen Netzwerkdienstes (z. B. E-Mail) oder den vorübergehenden Verlust aller Netzwerkverbindungen und -dienste. Im schlimmsten Fall kann beispielsweise eine Website, auf die täglich Millionen Benutzer zugreifen, zeitweise gezwungen sein, ihren Betrieb einstellen. Bei einem DoS-Angriff können auch Programme und Dateien in einem Computersystem zerstört werden. Auch wenn DoS-Angriffe meist absichtlich und böswillig sind, können sie manchmal auch unbeabsichtigt passieren. Ein DoS-Angriff stellt eine Art von Sicherheitsverletzung dar, die meist nicht zu einem Diebstahl von Informationen oder anderen Sicherheitsverlusten führt. Trotzdem können solche Angriffe für die Zielperson bzw. das geschädigte Unternehmen mit einem beträchtlichen Zeitaufwand und erheblichen Kosten verbunden sein.

Drahtloser Adapter

Enthält die Schaltkreise, mit denen ein Computer oder ein anderes Gerät mit einem (an einem drahtlosen Netzwerk angeschlossenen) drahtlosen Router kommunizieren kann. Drahtlose Adapter können entweder im Hauptschaltkreis eines Hardwaregeräts integriert sein oder sich auf einer separaten Zusatzkarte befinden, die in den entsprechenden Anschluss eines Gerätes eingesteckt wird.

E

ESS (Extended Service Set)

Eine Gruppe von mindestens zwei Netzwerken, die ein Subnetz bilden.

F

Firewall

Ein System, das dazu dient, nicht autorisierte Zugriffe auf ein bzw. aus einem privaten Netzwerk zu verhindern. Firewalls können in Form von Hardware, Software oder einer Kombination von beiden implementiert werden. Sie werden häufig verwendet, um zu verhindern, dass nicht autorisierte Internetbenutzer auf private Netzwerke (insbesondere Intranets) zugreifen, die mit dem Internet verbunden sind. Alle Nachrichten, die in das Intranet gelangen oder dieses verlassen, verlaufen durch eine Firewall. Von dieser werden alle Nachrichten überprüft und jene blockiert, die nicht die angegebenen Sicherheitskriterien erfüllen. Firewalls werden als erste Verteidigungslinie beim Schutz privater Informationen betrachtet. Zur höheren Sicherheit können die Daten verschlüsselt werden.

G

Gemeinsamer geheimer Schlüssel

Siehe auch RADIUS. Schützt den sensiblen Teil von RADIUS-Nachrichten. Der gemeinsame geheime Schlüssel ist ein Kennwort, das von dem Authentifikator und dem Authentifizierungsserver auf eine bestimmte sichere Weise gemeinsam verwendet wird.

H

Hotspot

Ein bestimmter örtlicher Standort, an dem ein Zugriffspunkt mobilen Besuchern den Zugriff auf öffentliche Breitband-Netzwerkdienste über ein drahtloses Netzwerk ermöglicht. Hotspots befinden sich oft in der Nähe von stark frequentierten Einrichtungen, z. B. Flughäfen, Bahnhöfen, Bibliotheken, Jachthäfen, Messe-Centern und Hotels. Sie haben meist eine geringe Reichweite.

I

Integriertes Gateway

Ein Gerät, in dem die Funktionen eines Zugriffspunkts, Routers und einer Firewall kombiniert sind. Einige Geräte können auch Sicherheitsoptimierungen und Überbrückungsfunktionen enthalten.

IP-Adresse

Ein Bezeichner für einen Computer oder ein Gerät in einem TCP/IP-Netzwerk. Netzwerke, die das TCP/IP-Protokoll verwenden, leiten Nachrichten anhand der IP-Adresse des Ziels weiter. Das Format einer IP-Adresse besteht aus einer numerischen 32 Bit-Adresse, die in Form von vier, durch Punkte getrennte Zahlen geschrieben wird. Jede Zahl kann zwischen 0 und 255 liegen. Eine IP-Adresse kann zum Beispiel so aussehen: 192.168.1.100.

IP-Spoofing

Das Fälschen der IP-Adressen in einem IP-Paket. Dieses Methode wird in vielen Arten von Angriffen einschließlich dem "Session-Hijacking" verwendet. Sie wird oftmals auch dazu verwendet, die Kopfzeilen von SPAM-E-Mails zu fälschen, damit diese E-Mails nicht mehr zurückverfolgt werden können.

J

K

Klartext

Nachrichten, die nicht verschlüsselt sind.

L

LAN (Local Area Network)

Ein Computernetzwerk, dass sich über ein relativ kleines Gebiet erstreckt. Die meisten LANs sind auf ein einzelnes Gebäude oder eine Gruppe von Gebäuden eingeschränkt. Per Telefonverbindungen oder Funkwellen kann ein LAN aber auch über eine beliebige Entfernung mit anderen LANs verbunden werden. Ein System aus LANs, die auf diese Weise miteinander verbunden sind, wird WAN (Wide-Area Network) genannt.

In den meisten LANs werden Workstations und PCs über normale Hubs oder Switches miteinander verbunden. Jeder Knoten (ein einzelner Computer) in einem LAN hat seine eigene CPU, mit der er Programme ausführt, kann aber auch auf Daten und Geräte (z. B. Drucker) im LAN zugreifen. Auf diese Weise können teure Geräte (z. B. Laserdrucker) sowie Daten von vielen Benutzern gemeinsam genutzt werden. Über ein LAN können Benutzer auch miteinander kommunizieren, z. B. E-Mails senden oder an Chat-Sitzungen teilnehmen.

M

MAC (Media Access Control oder Message Authenticator Code)

Für das erstgenannte von beiden siehe "MAC-Adresse". Die zweite ausgeschriebene Abkürzung (Message Authenticator Code) bezeichnet einen Code, der zum Identifizieren einer bestimmten Nachricht (z. B. einer RADIUS-Nachricht) verwendet wird. Der Code ist gewöhnlich ein kryptografisch starker Hash des Nachrichteninhalts, der einen eindeutigen Wert als Replay-Schutz enthält.

MAC-Adresse (Media Access Control Address)

Eine Adresse auf unterer Ebene, die einem physikalischen Gerät zugewiesen wird, das auf das Netzwerk zugreift.

"Man-in-the-Middle"-Angriff

Der Angreifer fängt Nachrichten bei einem öffentlichen Schlüsselaustausch ab und überträgt sie neu, wobei er den angeforderten Schlüssel durch deren eigene öffentliche Schlüssel ersetzt, so dass die beiden ursprünglichen Parteien weiterhin den Eindruck haben, direkt miteinander zu kommunizieren. Dabei verwendet der Angreifer ein Programm, dass sich dem Client gegenüber als Server und dem Server gegenüber als Client ausgibt. Der Angriff kann dazu dienen, einfach nur Zugriff auf die Nachrichten zu erhalten. Der Angreifer hat aber auch die Möglichkeit, die Nachrichten zu ändern, bevor er sie wieder weiterleitet. Der Begriff leitet sich von einem Ballspiel ab, bei dem mehrere Personen versuchen, sich gegenseitig den Ball zuzuwerfen, während ein einzelner Mitspieler in der Mitte versucht, den Ball abzufangen.

N

Netzwerk

Eine Gruppe von Zugriffspunkten und deren zugehörige Benutzer, gleichbedeutend einem ESS. Die Informationen über dieses Netzwerk werden in McAfee Wireless Home Network Security gepflegt. Siehe "ESS".

NIC (Network Interface Card, Netzwerkkarte)

Eine Karte, die in ein Notebook oder ein anderes Gerät gesteckt wird und das Gerät mit dem LAN verbindet.

Nicht autorisierter Zugriffspunkt

Ein Zugriffspunkt, den ein Unternehmen für den Betrieb nicht autorisiert. Das Problem dabei ist, dass nicht autorisierte Zugriffspunkte oft nicht den Sicherheitsrichtlinien für WLANs (Wireless LAN, Funk-LAN) entsprechen. Ein nicht autorisierter Zugriffspunkt bietet eine offene, unsichere Schnittstelle in das Unternehmensnetzwerk von außerhalb der physikalisch kontrollierten Einrichtung.

In einem ordnungsgemäß gesicherten WLAN richten nicht autorisierte Zugriffspunkte mehr Schäden an als nicht autorisierte Benutzer. Wenn wirksame Authentifizierungsmechanismen vorhanden sind, müssen nicht autorisierte Benutzer beim Versuch, auf ein WLAN zuzugreifen, nicht unbedingt auch an wertvolle Ressourcen des Unternehmens gelangen. Zu größeren Problemen kommt es jedoch, wenn sich ein Mitarbeiter oder Hacker über den nicht autorisierten Zugriffspunkt anmeldet. Ein nicht autorisierter Zugriffspunkt erlaubt praktisch jedem, der über ein 802.11-kompatibles Gerät verfügt, den Zutritt in das Unternehmensnetzwerk. Dadurch gelangt man schnell sehr nah an geschäftskritische Ressourcen.

O

P

PCI-Drahtlosadapter-Karte

Verbindet einen Desktopcomputer mit einem Netzwerk. Die Karte wird in einen PCI-Erweiterungssteckplatz im Computer gesteckt.

PPPoE

Abkürzung für "Point-to-Point Protocol Over Ethernet". PPPoE wird von vielen DSL-Providern verwendet und unterstützt die in PPP häufig verwendeten Protokollebenen und Authentifizierung. Mit PPPoE kann eine Punkt-zu-Punkt-Verbindung in der normalen Multipoint-Ethernet-Architektur hergestellt werden.

Protokoll

Ein vorab vereinbartes Format zum Übertragen von Daten zwischen zwei Geräten. Aus Sicht des Benutzers besteht der einzige interessante Aspekt bei Protokollen darin, dass der Computer oder das Gerät die entsprechenden Protokolle unterstützen muss, um mit einem jeweils anderen Computer kommunizieren zu können. Das Protokoll kann entweder in der Hardware oder in der Software implementiert sein.

Q

R

RADIUS (Remote Access Dial-In User Service)

Ein Protokoll zum Authentifizieren von Benutzern, meist im Zusammenhang mit Remote-Zugriff. Ursprünglich definiert für den Einsatz in RAS-Einwahl-Servern, wird das Protokoll heutzutage in einer breiten Vielzahl von Authentifizierungsumgebungen genutzt, einschließlich der 802.1x-Authentifizierung des gemeinsamen geheimen Schlüssels von WLAN-Benutzern.

Roaming

Die Fähigkeit, aus dem Empfangbereich eines Zugriffspunkts in den eines anderen zu wechseln, ohne dass dabei der Betrieb unterbrochen oder die Verbindung verloren wird.

Router

Ein Netzwerkgerät, das Pakete von einem Netzwerk in ein anderes weiterleitet. Router lesen jedes eingehende Paket und entscheiden anhand interner Routingtabellen, wie das Paket weitergeleitet werden soll. Die Wahl der Schnittstelle, an die ausgehende Pakete gesendet werden, kann davon abhängen, in welcher Konstellation Quell- und Zieladresse miteinander stehen, oder sich nach den aktuellen Gegebenheiten im Netzwerkverkehr (z. B. Auslastung, Leitungskosten oder ausgefallene Leitungen) richten. Für "Router" wird manchmal auch der Begriff "Zugriffspunkt" verwendet.

S

Schlüssel

Eine Folge von Buchstaben und/oder Zahlen, mit der zwei Geräte ihre Kommunikation miteinander authentifizieren können. Dabei müssen beide Geräte über den Schlüssel verfügen. Siehe auch "WEP" und "WPA-PSK".

SSID (Service Set Identifier)

Der Netzwerkname für die Geräte in einem Funk-LAN-Subsystem. Das ist eine Zeichenfolge aus 32 Zeichen, die im Klartext steht und zum Kopf jedes WLAN-Pakets hinzugefügt wird. Die SSID unterscheidet WLANs voneinander. Daher müssen alle Benutzer eines Netzwerks dieselbe SSID angeben, um auf einen bestimmten Zugriffspunkt zuzugreifen. Mit einer SSID wird der Zugriff von Clientgeräten verhindert, die eine andere SSID besitzen. Die SSID wird jedoch von Zugriffspunkten standardmäßig zusammen mit dem Signal übertragen. Dadurch kann ein Hacker die SSID per "Sniffing" selbst dann ermitteln, wenn die SSID-Übertragung deaktiviert ist.

SSL (Secure Sockets Layer)

Ein von Netscape entwickeltes Protokoll zum Übermitteln vertraulicher Dokumente über das Internet. SSL arbeitet mit einem öffentlichen Schlüssel, mit dem die Daten verschlüsselt werden, die über die SSL-Verbindung übertragen werden. SSL wird sowohl von Netscape Navigator als auch von Internet Explorer genutzt und unterstützt. Viele Websites verwenden dieses Protokoll, wenn Benutzer vertrauliche Informationen (z. B. Kreditkartennummern) eingeben müssen. Laut Konvention beginnen URLs, die eine SSL-Verbindung erfordern, mit der Zeichenfolge "https:" anstelle von "http:".

T

TKIP (Temporal Key Integrity Protocol)

Eine schnelle Methode zum Lösen der konstruktionsbedingten Sicherheitsschwächen von WEP, speziell des Problems der Wiederverwendung von Verschlüsselungsschlüsseln. Bei TKIP werden temporäre Schlüssel nach jeweils 10.000 Paketen geändert. Auf diese Weise wird eine dynamische Verteilungsmethode erzielt, die die Sicherheit des Netzwerks beträchtlich erhöht. Der TKIP-Sicherheitsprozess beginnt mit einem temporären 128-Bit-Schlüssel, der von Clients und Zugriffspunkten gemeinsam verwendet wird. TKIP kombiniert diesen temporären Schlüssel mit der MAC-Adresse (des Clientcomputers) und fügt dann einen relativ großen Initialisierungsvektor (16 Oktetts) hinzu, um den Schlüssel zu erstellen, mit dem die Daten verschlüsselt werden. Durch diese Vorgehensweise wird sichergestellt, dass jede Station ihre Daten mit einem anderen Schlüssel-Stream verschlüsselt. TKIP führt die Verschlüsselung mit RC4 durch. WEP verwendet ebenfalls RC4.

U

USB-Drahtlosadapter-Karte

Eine erweiterbare serielle Schnittstelle mit Plug-and-Play-Funktionalität. Diese Schnittstelle bietet eine standardisierte und preisgünstige drahtlose Anschlussmöglichkeit für Peripheriegeräte wie Tastaturen, Mäuse, Joysticks, Drucker, Scanner, Speichergeräte und Videokameras.

V

Verschlüsselung

Die Umwandlung von Daten in einen geheimen Code. Verschlüsselung ist der wirkungsvollste Weg, Datensicherheit zu erzielen. Um eine verschlüsselte Datei lesen zu können, ist Zugriff auf den geheimen Schlüssel bzw. das Kennwort erforderlich, mit dem die Daten entschlüsselt werden können. Unverschlüsselte Daten bezeichnet man als Klartext; verschlüsselte Daten werden chiffrierter Text genannt.

VPN (Virtual Private Network)

Ein Netzwerk, das entsteht, indem Knoten unter Verwendung von öffentlichen Leitungen neu miteinander verbunden werden. Es gibt zum Beispiel eine Reihe von Systemen, mit denen Sie Netzwerke erstellen können, die das Internet als Medium für den Datentransport verwenden. Diese Systeme setzen Verschlüsselung und andere Sicherheitsmechanismen ein, um sicherzustellen, dass nur autorisierte Benutzer auf das Netzwerk zugreifen und die Daten nicht abgefangen werden können.

W

Wardriver

Das sind mit Notebooks bewaffnete Eindringlinge, die mit spezieller Software und modifizierter Hardware durch die Gegend streifen, um Datenverkehr von Funk-LANs abzufangen.

WEP (Wired Equivalent Privacy)

Ein Verschlüsselungs- und Authentifizierungsprotokoll aus dem Standard 802.11. Die anfänglichen Versionen basieren auf RC4-Verschlüsselungen und haben beträchtliche Schwächen. Der Sicherheitsansatz von WEP besteht darin, dass per Funk übertragene Daten verschlüsselt werden, damit sie geschützt sind, wenn sie von einem Endpunkt zum anderen übertragen werden. Es hat sich jedoch herausgestellt, dass WEP nicht so sicher ist, wie man ursprünglich angenommen hatte.

Wi-Fi (Wireless Fidelity)

Dieser Begriff wird allgemein für alle Arten von 802.11-kompatiblen Netzwerken verwendet, sei es 802.11b, 802.11a, Dual-Band, usw. Der Begriff wird von der Wi-Fi Alliance verwendet.

Wi-Fi Alliance

Eine Organisation, die aus führenden Anbietern von drahtloser Hardware und Software besteht und deren Ziel darin liegt, (1) allen 802.11-basierten Produkten die gegenseitige Kompatibilität zu zertifizieren, und (2) den Begriff "Wi-Fi" in allen Märkten für Produkte für 802.11-basierte Funk-LANs als globalen Markennamen zu fördern. Die Organisation dient als Konsortium, Testlabor und Clearinghouse für Anbieter, die die gegenseitige Kompatibilität und das Wachstum dieser Branche voranbringen möchten.

Auch wenn alle Produkte der Standards 802.11a/b/g als Wi-Fi bezeichnet werden, dürfen nur die Produkte, die den Test der Wi-Fi Alliance bestanden haben, das Prädikat "Wi-Fi Certified" (eine eingetragene Marke) tragen. Produkte, die den Test erfolgreich bestanden haben, müssen ein Identifikationssiegel auf ihrer Verpackung haben, auf dem "Wi-Fi Certified" sowie das verwendete Funkfrequenzband stehen. Die Wi-Fi Alliance war früher unter der Bezeichnung Wireless Ethernet Compatibility Alliance (WECA) bekannt, änderte jedoch im Oktober 2002 ihren Namen, um die Marke "Wi-Fi" besser darstellen zu können, deren Aufbau das Ziel der Gruppe ist.

Wi-Fi Certified

Produkte, die von der Wi-Fi Alliance getestet und als Wi-Fi Certified (eine eingetragene Marke) zugelassen wurden, sind als miteinander vollständig kompatibel zertifiziert, auch wenn sie von unterschiedlichen Herstellern stammen. Ein Benutzer eines Produkts mit dem Prädikat "Wi-Fi Certified" kann einen Zugriffspunkt einer beliebigen Marke zusammen mit Clienthardware anderer Marken, die ebenfalls zertifiziert sind, verwenden. Üblicherweise funktionieren Wi-Fi-Produkte mit allen anderen Produkten zusammen, die dieselbe Funkfrequenz verwenden (z. B. 2,4 GHz bei 802.11b oder 11g; 5 GHZ bei 802.11a), auch wenn diese nicht das Prädikat "Wi-Fi Certified" haben.

WLAN (Wireless Local Area Network)

Siehe auch LAN. Ein LAN, das ein drahtloses Medium zum Verbinden verwendet. In WLANs erfolgt die Kommunikation zwischen den Knoten über hochfrequente Funkwellen anstelle von Kabeln.

Wörterbuchangriff

Bei diesen Angriffen wird versucht, ein Kennwort zu ermitteln, indem unzählige Wörter aus einer Liste durchprobiert werden. Dabei geben die Angreifer diese Wörter und alle ihre Kombinationen nicht selbst manuell ein, bis sie das Kennwort von jemandem ermittelt haben, sondern verwenden dafür Tools, die diesen Vorgang automatisieren.

WPA (Wi-Fi Protected Access)

Ein Spezifikationsstandard, der das Niveau von Datenschutz und Zugriffskontrolle bei vorhandenen und zukünftigen Funk-LAN-Systemen stark erhöht. WPA ist vom Standard IEEE 802.11i abgeleitet und damit kompatibel und für die Ausführung auf vorhandener Hardware in Form eines Softwareupgrade entworfen. Bei korrekter Installation bietet es Benutzern von Funk-LANs ein hohes Maß an Sicherheit dafür, dass ihre Daten geschützt bleiben und nur autorisierte Netzwerkbenutzer auf das Netzwerk zugreifen können.

WPA-PSK

Ein spezieller WPA-Modus, der für Privatanwender entworfen wurde, die keine starke Sicherheit wie in Unternehmen üblich benötigen und keinen Zugriff auf Authentifizierungsserver haben. In diesem Modus kann der Privatanwender das Startkennwort manuell eingeben, um WPA im PSK-Modus zu aktivieren, und sollte die Passphrase auf jedem drahtlosen Computer und Zugriffspunkt regelmäßig ändern. Siehe auch TKIP.

X

Y

Z

Zugriffspunkt

Ein Netzwerkgerät, das 802.11-kompatiblen Clients die Verbindung zu einem LAN (Local Area Network) ermöglicht. Zugriffspunkte erweitern die physikalische Betriebsreichweite für drahtlose Benutzer. Sie werden auch als drahtlose Router bezeichnet.

McAfee VirusScan 3

Willkommen bei McAfee VirusScan.

McAfee VirusScan ist ein Antiviren-Abonnementservice, der Ihnen umfassenden, zuverlässigen und stets aktuellen Virenschutz bietet. Unterstützt durch die preisgekrönte McAfee-Scantechnologie schützt VirusScan vor Viren, Würmern, Trojanern, verdächtigen Skripts, Hybridangriffen und anderen Bedrohungen.

Das Programm umfasst folgende Funktionen:

ActiveShield – Überprüft alle Dateien, wenn auf sie von Ihnen oder Ihrem Computer zugegriffen wird.

Prüfen – Durchsucht Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und anderen Bedrohungen.

Quarantäne – Verschlüsselt und isoliert verdächtige Dateien vorübergehend im Quarantäneordner, bis eine entsprechende Aktion durchgeführt werden kann.

Erkennung feindseliger Aktivitäten – Überwacht den Computer auf virenähnliche Aktivitäten, die durch Würmer und verdächtige Skripts verursacht werden.

Neue Funktionen

Diese Version von VirusScan enthält folgende neue Funktionen:

- **Erkennen und Entfernen von Spyware und Adware**
  VirusScan identifiziert und entfernt Spyware, Adware und andere Programme, die Ihre Privatsphäre gefährden und die Leistung Ihres Computers beeinträchtigen.
- **Tägliche automatische Updates**
  Tägliche automatische VirusScan-Updates schützen Sie vor den neuesten identifizierten und nicht identifizierten Computerbedrohungen.
- **Schnelles Scannen im Hintergrund**
  Schnelle, im Hintergrund ausgeführte Scans identifizieren und zerstören Viren, Trojaner, Spyware, Adware, Einwählprogramme und andere Bedrohungen, ohne Sie bei der Arbeit zu unterbrechen.
- **Echtzeit-Sicherheitswarnungen**
  Sicherheitswarnungen benachrichtigen Sie über den Ausbruch neuer Viren und Sicherheitsbedrohungen. Außerdem bieten sie Ihnen die Möglichkeit, diese Bedrohungen zu entfernen, zu neutralisieren oder weitere Informationen dazu anzuzeigen.

- **Erkennen und Bereinigen an den am meisten gefährdeten Stellen**
  VirusScan führt die Überwachung und Bereinigung überall dort durch, wo Computer am meisten gefährdet sind: E-Mails, Instant Messaging-Anlagen und Internetdownloads.
- **Überwachen von E-Mails auf wurmähnliche Aktivitäten**
  WormStopper™ überwacht verdächtiges Verhalten, das bei massenhaft versandten E-Mails charakteristisch ist, und verhindert so, dass sich Viren und Würmer per E-Mail auf andere Computer ausbreiten können.
- **Überwachen von Skripts auf wurmähnliche Aktivitäten**
  ScriptStopper™ überwacht den Computer auf verdächtige Skriptausführungen und verhindert, dass sich Viren und Würmer per E-Mail auf andere Computer ausbreiten.
- **Kostenloser technischer Support per Instant Messaging und E-Mail**
  Der live bereitgestellte technische Support bietet leicht zugängliche und schnelle Beratung mithilfe von Instant Messaging und E-Mail.

Testen von VirusScan

Bevor Sie VirusScan zum ersten Mal verwenden, sollten Sie Ihre Installation testen. Gehen Sie für das separate Testen der ActiveShield- und Scan-Funktionen wie nachfolgend beschrieben vor.

Testen von ActiveShield

HINWEIS
Klicken Sie zum Testen von ActiveShield in SecurityCenter in der Registerkarte **VirusScan** auf **VirusScan testen**, um eine Online-Support-FAQ mit den folgenden Schritten anzuzeigen.

So testen Sie ActiveShield:

1. Rufen Sie http://www.eicar.com/ in Ihrem Webbrowser auf.
2. Klicken Sie auf den Link **The AntiVirus testfile eicar.com** (Die AntiVirus-Testdatei eicar.com).
3. Führen Sie einen Bildlauf zum unteren Ende der Seite durch. Unter **Download** werden vier Links angezeigt.
4. Klicken Sie auf **eicar.com**.

Wenn ActiveShield korrekt ausgeführt wird, wird die Datei **eicar.com** sofort als Virus erkannt, nachdem Sie auf den Link geklickt haben. Wenn Sie sehen möchten, wie ActiveShield mit möglichen Bedrohungen umgeht, können Sie versuchen, entdeckte Dateien zu löschen oder zu isolieren. Nähere Informationen dazu finden Sie unter *Grundlegendes zu Sicherheitswarnungen* auf Seite 68.

Testen von Scan

Bevor Sie Scan testen können, müssen Sie ActiveShield deaktivieren, damit die Testdateien nicht von ActiveShield erkannt werden, bevor Scan sie erkennen kann. Laden Sie anschließend die Testdateien herunter.

So laden Sie die Testdateien herunter:

1. Deaktivieren Sie ActiveShield: Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Deaktivieren**.
2. Laden Sie die EICAR-Testdateien von der EICAR-Website herunter:
   a. Rufen Sie http://www.eicar.com/ auf.
   b. Klicken Sie auf den Link **The AntiVirus testfile eicar.com** (Die AntiVirus-Testdatei eicar.com).
   c. Führen Sie einen Bildlauf zum unteren Ende der Seite durch. Unter **Download** werden die folgenden Links angezeigt:

      eicar.com enthält eine Textzeile, die von VirusScan als Virus erkannt wird.

      eicar.com.txt (optional) ist dieselbe Datei, jedoch mit einem anderen Dateinamen. Diese Datei ist für diejenigen Benutzer vorgesehen, die mit dem ersten Link Probleme haben. Benennen Sie die Datei nach dem Download einfach in "eicar.com" um.

      eicar_com.zip ist eine Kopie des Testvirus in einer mit WinZip™ komprimierten ZIP-Datei (ein WinZip-Dateiarchiv).

      eicarcom2.zip ist eine Kopie des Testvirus in einer mit WinZip komprimierten ZIP-Datei, die sich ihrerseits in einer mit WinZip komprimierten ZIP-Datei befindet.

   d. Klicken Sie auf den jeweiligen Link, um die zugehörige Datei herunterzuladen. Für jede Datei wird ein Dialogfeld **Dateidownload** angezeigt.

e Klicken Sie auf **Speichern** und auf die Schaltfläche **Neuen Ordner erstellen**, und benennen Sie den Ordner anschließend in **VSO-Scan-Ordner** um.

f Doppelklicken Sie auf **VSO-Scan-Ordner**, und klicken Sie dann in jedem Dialogfeld **Speichern unter** wieder auf **Speichern**.

3 Wenn Sie die Dateien heruntergeladen haben, schließen Sie Internet Explorer.

4 Aktivieren Sie ActiveShield: Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Aktivieren**.

So testen Sie Scan:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Scan**.

2 Wechseln Sie in der Verzeichnisstruktur im linken Fensterbereich des Dialogfeldes zum **VSO-Scan-Ordner**, in dem Sie die Dateien gespeichert haben:

a Klicken Sie auf das Pluszeichen (**+**) neben dem Symbol für das Laufwerk C.

b Klicken Sie auf den **VSO-Scan-Ordner**, um ihn zu markieren (klicken Sie nicht auf das Pluszeichen **+** neben dem Ordner).

Dadurch wird Scan angewiesen, nur diesen Ordner zu überprüfen. Eine noch überzeugendere Demonstration der Fähigkeiten von Scan erhalten Sie, wenn Sie die Dateien an zufällig ausgewählten Standorten auf der Festplatte speichern.

3 Vergewissern Sie sich im Bereich **Prüfoptionen** des Dialogfeldes **Scan**, dass alle Optionen aktiviert sind.

4 Klicken Sie unten rechts im Dialogfeld auf **Prüfen**.

VirusScan durchsucht den **VSO-Scan-Ordner**. Die EICAR-Testdateien, die Sie in diesem Ordner gespeichert haben, werden in der **Liste der erkannten Dateien** aufgeführt. Wenn dies geschieht, wissen Sie, dass Scan einwandfrei funktioniert.

Wenn Sie sehen möchten, wie Scan mit möglichen Bedrohungen umgeht, können Sie versuchen, entdeckte Dateien zu löschen oder zu isolieren. Nähere Informationen dazu finden Sie unter *Grundlegendes zu Bedrohungserkennungen* auf Seite 78.

Verwenden von McAfee VirusScan

In diesem Abschnitt wird beschrieben, wie VirusScan verwendet wird.

Verwenden von ActiveShield

Nachdem ActiveShield gestartet (in den Computerspeicher geladen) und aktiviert wurde, bietet das Programm konstanten Schutz für Ihren Computer. ActiveShield durchsucht alle Dateien, auf die Sie oder Ihr Computer zugreifen. Wenn ActiveShield eine Datei entdeckt, versucht es automatisch, sie zu bereinigen. Wenn ActiveShield den Virus nicht bereinigen kann, können Sie die Datei isolieren oder löschen.

Aktivieren oder Deaktivieren von ActiveShield

Sobald Sie Ihren Computer nach Abschluss des Installationsvorgangs neu starten, wird ActiveShield standardmäßig gestartet (in den Computerspeicher geladen) und aktiviert (erkennbar am roten Symbol in der Windows-Taskleiste).

Ist ActiveShield angehalten (nicht geladen) oder deaktiviert (erkennbar am schwarzen Symbol), können Sie das Programm manuell starten oder auch so konfigurieren, dass das Programm bei jedem Start von Windows automatisch ausgeführt wird.

Aktivieren von ActiveShield

So aktivieren Sie ActiveShield nur für die aktuelle Windows-Sitzung:

Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Aktivieren**. Die Farbe des McAfee-Symbols ändert sich zu rot ().

Wenn ActiveShield weiterhin so konfiguriert ist, dass das Programm bei jedem Start von Windows ausgeführt wird, informiert Sie eine Nachricht, dass Ihr Computer jetzt vor Bedrohungen geschützt ist. Andernfalls wird ein Dialogfeld geöffnet, in dem Sie ActiveShield so konfigurieren können, dass das Programm bei jedem Start von Windows ausgeführt wird (Abbildung 3-1 auf Seite 58).

Deaktivieren von ActiveShield

So deaktivieren Sie ActiveShield nur für die aktuelle Windows-Sitzung:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Deaktivieren**.
2. Klicken Sie zur Bestätigung auf **Ja**.

   Die Farbe des McAfee-Symbols ändert sich zu schwarz ().

Wenn ActiveShield so konfiguriert ist, dass das Programm beim Starten von Windows automatisch ausgeführt wird, ist Ihr Computer nach einem Neustart wieder vor Bedrohungen geschützt.

Konfigurieren von ActiveShield-Optionen

Sie können die Start- und Scan-Optionen von ActiveShield in der Registerkarte **ActiveShield** im Dialogfeld **VirusScan - Optionen** (Abbildung 3-1) ändern, auf das Sie über das McAfee-Symbol in der Windows-Taskleiste zugreifen können.

McAfee VirusScan - Optionen
McAfee
virusscan
Hilfe
ActiveShield
Virus Map Melden
Geplanter Scanvorgang
Windows-Start
Starten Sie ActiveShield, wenn Windows gestartet wird (empfohlen)
Geben Sie an, ob Sie beim Starten des Computers geschützt sein möchten
E-Mails und Anlagen überprüfen
Geben Sie an, ob Sie beim Verwenden von E-Mail-Programmen geschützt sein möchten
Anlagen von eingehenden Instant Messages überprüfen
Geben Sie an, ob Sie beim Öffnen von Anlagen mit Hilfe von Instant Messaging-Programmen geschützt sein möchten
Erweitert
OK
Abbrechen
Übernehmen

Abbildung 3-1. ActiveShield-Optionen

Starten von ActiveShield

Sobald Sie Ihren Computer nach Abschluss des Installationsvorgangs neu starten, wird ActiveShield standardmäßig gestartet (in den Computerspeicher geladen) und aktiviert (gekennzeichnet durch das rote Symbol).

Wenn ActiveShield angehalten ist (erkennbar am schwarzen Symbol), können Sie das Programm so konfigurieren, dass es beim Starten von Windows automatisch ausgeführt wird (empfohlen).

HINWEIS

Beim Aktualisieren von VirusScan kann der **Update-Assistent** ActiveShield möglicherweise vorübergehend beenden, um neue Dateien zu installieren. Wenn Sie vom **Update-Assistenten** aufgefordert werden, auf **Fertig stellen** zu klicken, wird ActiveShield wieder gestartet.

So legen Sie fest, dass ActiveShield beim Starten von Windows automatisch ausgeführt wird:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

Das Dialogfeld **VirusScan-Optionen** wird geöffnet (Abbildung 3-1 auf Seite 58).

2 Aktivieren Sie das Kontrollkästchen **Starten Sie ActiveShield, wenn Windows gestartet wird (empfohlen)**, und klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

3 Klicken Sie zur Bestätigung auf **OK** und anschließend erneut auf **OK**.

Anhalten von ActiveShield

ACHTUNG
Wenn Sie ActiveShield anhalten, ist Ihr Computer nicht mehr vor Bedrohungen geschützt. Wenn Sie ActiveShield aus einem anderen Grund als einem Update anhalten müssen, sollten Sie sich vergewissern, dass Sie nicht mit dem Internet verbunden sind.

So legen Sie fest, dass ActiveShield beim Starten von Windows nicht mit ausgeführt wird:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

Das Dialogfeld **VirusScan - Optionen** wird geöffnet (Abbildung 3-1 auf Seite 58).

2 Deaktivieren Sie das Kontrollkästchen **Starten Sie ActiveShield, wenn Windows gestartet wird (empfohlen)**, und klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

3 Klicken Sie zur Bestätigung auf **OK** und anschließend erneut auf **OK**.

Prüfen von E-Mails und Anlagen

Standardmäßig wird das Überprüfen und automatische Bereinigen von E-Mails mithilfe der Option **E-Mails und Anlagen überprüfen** (Abbildung 3-1 auf Seite 58) aktiviert.

Wenn diese Option aktiviert ist, sucht ActiveShield automatisch nach Viren und versucht, eingehende (POP3) und ausgehende (SMTP) entdeckte E-Mail-Nachrichten und -Anlagen für die gebräuchlichsten E-Mail-Clients zu bereinigen. Hierzu zählen:

- Microsoft Outlook Express 4.0 oder höher
- Microsoft Outlook 97 oder höher

- Netscape Messenger 4.0 oder höher
- Netscape Mail 6.0 oder höher
- Eudora Light 3.0 oder höher
- Eudora Pro 4.0 oder höher
- Eudora 5.0 oder höher
- Pegasus 4.0 oder höher

HINWEIS
Für die folgenden E-Mail-Clients wird E-Mail-Überprüfung nicht unterstützt: Webbasierte E-Mail-Clients, IMAP-, AOL-, POP3 SSL- und Lotus Notes-Clients. E-Mail-Anlagen werden beim Öffnen jedoch von ActiveShield geprüft.

Wenn Sie die Option **E-Mails und Anlagen überprüfen** deaktivieren, werden die E-Mail-Scan-Optionen und die WormStopper-Optionen (Abbildung 3-2 auf Seite 61) automatisch deaktiviert. Wenn Sie das Überprüfen ausgehender E-Mails deaktivieren, werden die WormStopper-Optionen automatisch deaktiviert.

Wenn Sie die E-Mail-Scan-Optionen ändern, müssen Sie anschließend das E-Mail-Programm neu starten, damit die Änderungen wirksam werden.

Eingehende E-Mails

Wenn eine eingehende E-Mail-Nachricht oder Anlage entdeckt wird, führt ActiveShield folgende Schritte durch:

- Es wird versucht, die entdeckte E-Mail zu bereinigen.
- Es wird versucht, E-Mails, die nicht bereinigt werden können, zu isolieren oder zu löschen.
- Es wird eine Warnungsdatei in die eingehende E-Mail eingefügt, die Informationen über die Aktionen enthält, die zum Entfernen der möglichen Bedrohung durchgeführt wurden.

Ausgehende E-Mails

Wenn eine ausgehende E-Mail-Nachricht oder Anlage entdeckt wird, führt ActiveShield folgende Schritte durch:

- Es wird versucht, die entdeckte E-Mail zu bereinigen.
- Es wird versucht, E-Mails, die nicht bereinigt werden können, zu isolieren oder zu löschen.

HINWEIS
Einzelheiten zu Fehlermeldungen bei der Prüfung ausgehender E-Mails finden Sie in der Online-Hilfe.

Deaktivieren der Überprüfung von E-Mails

Standardmäßig werden von ActiveShield sowohl eingehende als auch ausgehende E-Mails überprüft. Sie können jedoch festlegen, dass ActiveShield nur eingehende oder nur ausgehende E-Mails überprüfen soll.

So deaktivieren Sie die Überprüfung von eingehenden oder ausgehenden E-Mails:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert**, und aktivieren Sie dann die Registerkarte **E-Mail** (Abbildung 3-2).
3. Deaktivieren Sie das Kontrollkästchen **Eingehende E-Mail-Nachrichten** bzw. **Ausgehende E-Mail-Nachrichten**, und klicken Sie dann auf **OK**.

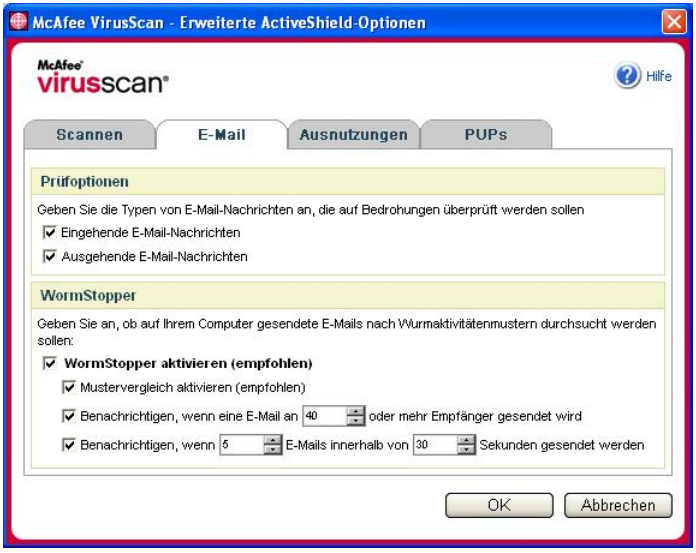


Abbildung 3-2. Erweiterte ActiveShield-Optionen – Registerkarte "E-Mail"

Prüfen auf Würmer

VirusScan überwacht Ihren Computer auf verdächtige Aktivitäten, die auf eine mögliche Gefahr auf Ihrem Computer hindeuten können. Während von VirusScan Viren und andere Bedrohungen bereinigt werden, verhindert dagegen WormStopper™, dass sich Viren und Würmern weiter ausbreiten können.

Computerwürmer sind sich selbst replizierende Viren, die sich im Arbeitsspeicher eines Computers befinden und Kopien von sich selbst per E-Mail verbreiten. Ohne WormStopper bemerken Sie Würmer möglicherweise erst, wenn deren Vervielfältigung immer mehr Systemressourcen in Anspruch nimmt, so dass die Leistung reduziert wird oder Tasks komplett angehalten werden.

Durch die Schutzmechanismen von WormStopper werden verdächtige Aktivitäten erkannt, gemeldet und blockiert. Folgende Vorgänge auf Ihrem Computer können als verdächtige Aktivitäten gelten:

- Wenn versucht wird, eine E-Mail an zahlreiche Adressen aus Ihrem Adressbuch weiterzuleiten
- Wenn versucht wird, mehrere E-Mails in schneller Abfolge weiterzuleiten

Wenn Sie ActiveShield so einstellen, dass im Dialogfeld **Erweiterte Optionen** die Standardoption **WormStopper aktivieren (empfohlen)** aktiviert ist, überwacht WormStopper E-Mail-Aktivitäten auf verdächtige Muster und benachrichtigt sie, wenn innerhalb eines festgelegten Zeitraums eine bestimmte Anzahl von E-Mails oder Empfängern überschritten wurde.

So stellen Sie ActiveShield zum Überprüfen von gesendeten E-Mail-Nachrichten auf wurmähnliche Aktivitäten ein:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **E-Mail**.
3. Klicken Sie auf **WormStopper aktivieren (empfohlen)** (Abbildung 3-3 auf Seite 63).

   Standardmäßig sind die folgenden Detailoptionen aktiviert:

   - Musterabgleich zum Erkennen verdächtiger Aktivitäten
   - Benachrichtigen, wenn eine E-Mail an 40 oder mehr Empfänger gesendet wird
   - Benachrichtigen, wenn 5 E-Mails innerhalb von 30 Sekunden gesendet werden

   HINWEIS
   Wenn Sie bei der Überwachung gesendeter E-Mails die Anzahl der Empfänger oder Sekunden ändern, führt dies möglicherweise zu fehlerhaften Erkennungen. Es wird empfohlen, auf **Nein** zu klicken, um die Standardeinstellung beizubehalten. Bei Bedarf können Sie jedoch auch **Ja** auswählen, um die Standardeinstellung auf die von Ihnen gewünschte Einstellung zu ändern.

Diese Option kann automatisch aktiviert werden, nachdem zum ersten Mal ein potenzieller Wurm entdeckt wurde (ausführliche Informationen dazu finden Sie unter *Verwalten potenzieller Würmer* auf Seite 69):

- Alle verdächtigen ausgehenden E-Mails automatisch blockieren

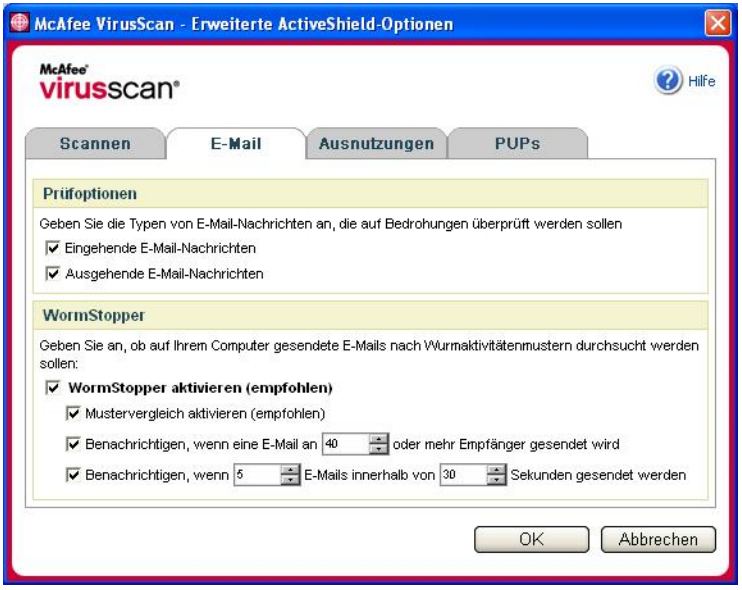


Abbildung 3-3. Erweiterte ActiveShield-Optionen – Registerkarte "E-Mail"

Prüfen der Anlagen von eingehenden Instant Messages

Standardmäßig wird die Überprüfung von Instant Messages-Anlagen mit der Option **Anlagen von eingehenden Instant Messages überprüfen** (Abbildung 3-1 auf Seite 58) aktiviert.

Wenn diese Option aktiviert ist, überprüft VirusScan automatisch die Anlagen von eingehenden Instant Messages der gängigsten Instant Messaging-Programme und versucht, entdeckte Dateien zu bereinigen. Folgende Programme werden unterstützt:

- MSN Messenger 6.0 oder höher
- Yahoo Messenger 4.1 oder höher
- AOL Instant Messenger 2.1 oder höher

HINWEIS

Aus Sicherheitsgründen kann die automatische Bereinigung von Instant Messaging-Anlagen nicht deaktiviert werden.

Wenn eine eingehende Instant Messaging-Anlage entdeckt wird, führt VirusScan die folgenden Schritte aus:

- Es versucht, die entdeckte Nachricht zu bereinigen.
- Bei einer Nachricht, die nicht bereinigt werden kann, fragt das Programm nach, ob Sie die Nachricht löschen oder isolieren möchten.

Prüfen aller Dateien

Wenn Sie in ActiveShield die Standardeinstellung **Alle Dateien (empfohlen)** verwenden, werden Dateien aller Typen überprüft, wenn der Computer auf sie zugreift. Mit dieser Option erhalten Sie die gründlichste Überprüfung, die möglich ist.

So stellen Sie ActiveShield zum Überprüfen aller Dateitypen ein:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **Scannen** (Abbildung 3-4).
3. Klicken Sie auf **Alle Dateien (empfohlen)** und dann auf **OK**.

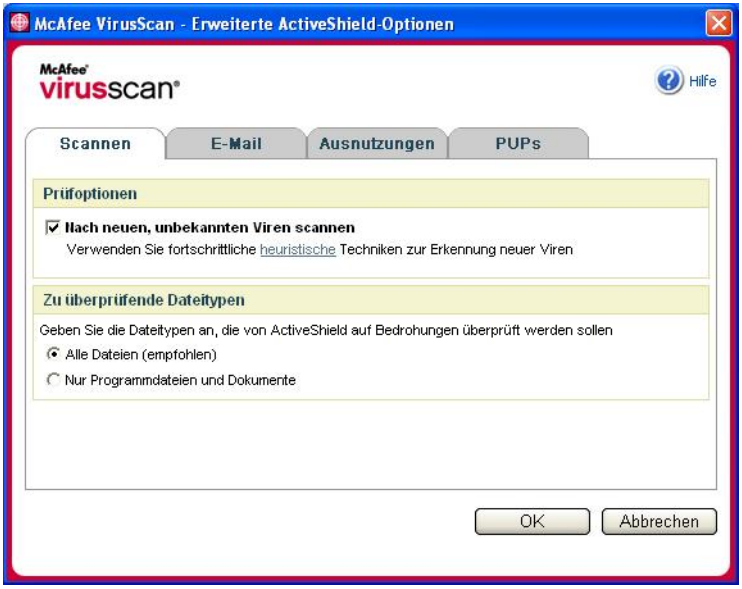


Abbildung 3-4. Erweiterte ActiveShield-Optionen – Registerkarte "Scannen"

Ausschließliches Prüfen von Programmdateien und Dokumenten

Wenn Sie in ActiveShield die Option **Nur Programmdateien und Dokumente** aktivieren, werden ausschließlich Programmdateien und Dokumente überprüft. Andere von Ihrem Computer verwendete Dateien werden in diesem Fall nicht durchsucht. Welche Dateitypen ActiveShield überprüft, wird von der jeweils neuesten Virensignaturdatei (DAT-Datei) bestimmt. So legen Sie fest, dass ActiveShield nur Programmdateien und Dokumente überprüft:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **Scannen** (Abbildung 3-4 auf Seite 64).
3. Klicken Sie auf **Nur Programmdateien und Dokumente** und dann auf **OK**.

Prüfen auf neue, unbekannte Viren

Wenn Sie ActiveShield so konfigurieren, dass die Standardoption **Nach neuen, unbekannten Viren scannen** verwendet wird, versucht das Programm mithilfe von erweiterten heuristischen Techniken, in den Dateien Muster zu finden, die mit Signaturen bekannter Viren übereinstimmen, oder die zumindest ein Indiz für einen noch unbekannten Virus sein könnten.

So stellen Sie ActiveShield zum Überprüfen auf neue, unbekannte Viren ein:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **Scannen** (Abbildung 3-4 auf Seite 64).
3. Klicken Sie auf **Nach neuen, unbekannten Viren scannen** und dann auf **OK**.

Prüfen auf Skripts

VirusScan überwacht Ihren Computer auf verdächtige Aktivitäten, die auf eine mögliche Gefahr auf Ihrem Computer hindeuten können. Während VirusScan Viren und andere Bedrohungen bereinigt, verhindert ScriptStopper™, dass Trojaner Skripts ausführen, mit denen Viren weiterverbreitet werden.

Ein Trojaner ist ein verdächtiges Programm, das als nützliche Anwendung getarnt ist. Trojaner sind keine Viren, da sie sich nicht fortpflanzen, können Ihrem Computer jedoch einen ähnlich Schaden zufügen wie Viren.

Durch den Schutzmechanismen von ScriptStopper werden verdächtige Aktivitäten erkannt, gemeldet und blockiert. Der folgende Vorgang auf Ihrem Computer kann als verdächtige Aktivität gelten:

- Die Ausführung eines Skripts, das zur Folge hat, dass Dateien erstellt, kopiert oder gelöscht werden, oder dass Ihre Windows-Registrierung geöffnet wird.

Wenn Sie ActiveShield so einstellen, dass die Standardoption **ScriptStopper aktivieren (empfohlen)** im Dialogfeld **Erweiterte Optionen** aktiviert ist, überwacht ScriptStopper ausgeführte Skripts auf verdächtige Muster und benachrichtigt Sie, wenn innerhalb eines festgelegten Zeitraums eine bestimmte Anzahl von E-Mails oder Empfängern überschritten wurde.

So stellen Sie ActiveShield zum Überprüfen von ausgeführten Skripts auf wurmähnliche Aktivitäten ein:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **Ausnutzungen** (Abbildung 3-5).
3. Klicken Sie auf **ScriptStopper aktivieren (empfohlen)** und dann auf **OK**.

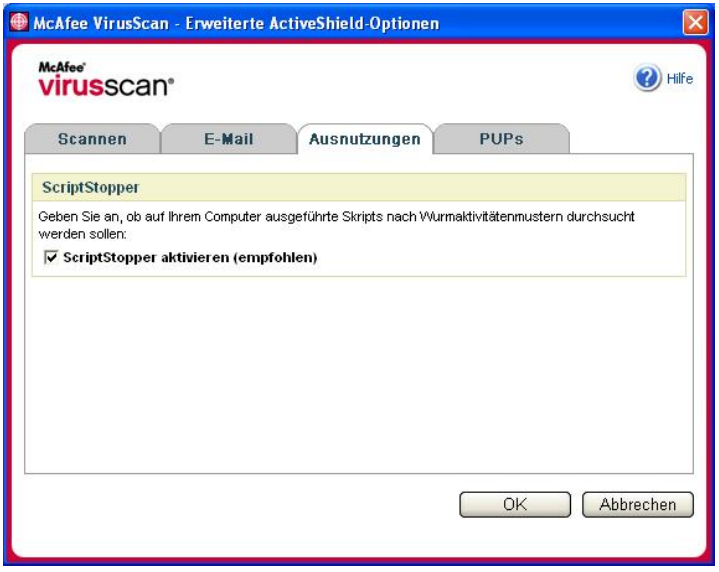


Abbildung 3-5. Erweiterte ActiveShield-Optionen – Registerkarte "Ausnutzungen"

Prüfen auf potenziell unerwünschte Programme (PUP)

HINWEIS
Wenn auf Ihrem Computer McAfee AntiSpyware installiert ist, verwaltet es alle Aktivitäten von potenziell unerwünschten Programmen. Öffnen Sie McAfee AntiSpyware, um die gewünschten Optionen zu konfigurieren.

Wenn Sie ActiveShield so konfigurieren, dass die standardmäßige Option **Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)** im Dialogfeld **Erweiterte Optionen** aktiviert ist, werden Spyware, Adware und andere Programme, die Ihre persönlichen Daten sammeln und ohne Ihre Zustimmung weiterleiten, von der entsprechenden Schutzfunktion rasch entdeckt, blockiert und entfernt.

So stellen Sie ActiveShield zum Überprüfen auf potenziell unerwünschte Programme (PUP) ein:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **PUPs** (Abbildung 3-6).
3. Klicken Sie auf **Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)** und dann auf **OK**.

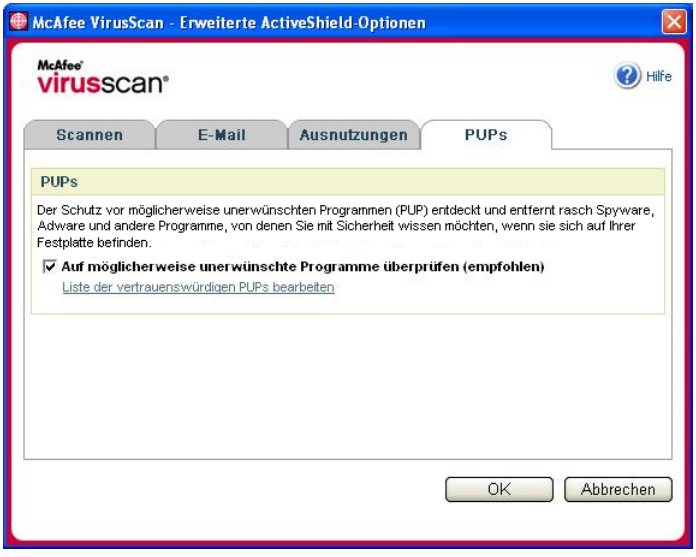

McAfee VirusScan - Erweiterte ActiveShield-Optionen
McAfee
virusscan
Hilfe
Scannen
E-Mail
Ausnutzungen
PUPs
PUPs
Der Schutz vor möglicherweise unerwünschten Programmen (PUP) entdeckt und entfernt rasch Spyware, Adware und andere Programme, von denen Sie mit Sicherheit wissen möchten, wenn sie sich auf Ihrer Festplatte befinden.
Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)
Liste der vertrauenswürdigen PUPs bearbeiten
OK
Abbrechen

Abbildung 3-6. Erweiterte ActiveShield-Optionen – Registerkarte "PUPs"

Grundlegendes zu Sicherheitswarnungen

Wenn ActiveShield einen Virus findet, wird eine Viruswarnung ähnlich wie in Abbildung 3-7 angezeigt. Bei den meisten Viren, Trojanern und Würmern versucht ActiveShield automatisch, die Datei zu bereinigen, und zeigt eine Warnung an. Bei potenziell unerwünschten Programmen (PUP) wird die Datei von ActiveShield ermittelt, automatisch blockiert und eine Warnung angezeigt.

McAfee VirusScan
Virus gefunden
Die Datei C:\Dokumente und Einstellungen\Administrator\Lokale Einstell... ist mit dem Virus EICAR test file infiziert und kann nicht gereinigt werden.
Ich möchte...
Erkannte Datei löschen
Erkannte Datei unter Quarantäne stellen
Weitere Informationen
Aktuelle Tätigkeit fortsetzen

Abbildung 3-7. Viruswarnung

Anschließend können Sie auswählen, wie mit entdeckten Dateien und E-Mails, verdächtigen Skripts, potenziellen Würmern oder unerwünschten Programmen umgegangen werden soll. Sie haben auch die Möglichkeit, entdeckte Dateien zur näheren Prüfung an das McAfee AVERT-Labor zu senden.

Zur zusätzlichen Sicherheit werden Sie aufgefordert, ihren gesamten Computer umgehend zu überprüfen, wenn ActiveShield eine verdächtige Datei entdeckt. Solange Sie diese Aufforderung nicht ausblenden, werden Sie in regelmäßigen Abständen immer wieder erinnert, bis Sie die Überprüfung durchführen.

Verwalten entdeckter Dateien

1. Wenn ActiveShield die Datei bereinigen kann, können Sie weitere Informationen anzeigen oder die Warnung ignorieren:
   - Klicken Sie auf **Weitere Informationen**, um den Namen, Speicherort und zugehörigen Virusnamen der entdeckten Datei anzuzeigen.
   - Klicken Sie auf **Aktuelle Tätigkeit fortsetzen**, um die Warnung zu ignorieren und zu schließen.
2. Wenn ActiveShield die Datei nicht bereinigen kann, klicken Sie auf **Erkannte Datei unter Quarantäne stellen**, um verdächtige Dateien zu verschlüsseln und vorübergehend im Quarantäneverzeichnis zu isolieren, bis eine angemessene Maßnahme ergriffen werden kann.

Eine Meldung wird angezeigt, in der Sie aufgefordert werden, Ihren Computer auf Bedrohungen zu überprüfen. Klicken Sie auf **Scan**, um den Quarantänevorgang abzuschließen.

3 Wenn ActiveShield die Datei nicht isolieren kann, klicken Sie auf **Erkannte Datei löschen**, um die Datei zu entfernen.

Verwalten entdeckter E-Mails

Standardmäßig wird beim Überprüfen von E-Mails automatisch versucht, entdeckte E-Mails zu bereinigen. Sie werden in einer in der eingehenden Nachricht enthaltenen Warnungsdatei darüber informiert, ob die E-Mail bereinigt, isoliert oder gelöscht wurde.

Verwalten verdächtiger Skripts

Wenn ActiveShield ein verdächtiges Skript erkennt, können Sie weitere Informationen anzeigen und das Skript dann anhalten, wenn Sie nicht möchten, dass es initialisiert wird:

- Klicken Sie auf **Weitere Informationen**, um den Namen, den Speicherort und die Beschreibung der mit dem verdächtigen Skript verbundenen Aktivität anzuzeigen.
- Mit **Dieses Skript anhalten** können Sie die Ausführung des verdächtigen Skripts unterbinden.

Wenn Sie sicher sind, dass das Skript vertrauenswürdig ist, können Sie die Ausführung des Skripts zulassen:

- Klicken Sie auf **Gesamtes Skript zu diesem Zeitpunkt zulassen**, um zu erlauben, dass alle in einer einzelnen Datei enthaltenen Skripts in diesem bestimmten Fall ausgeführt werden.
- Klicken Sie auf **Aktuelle Tätigkeit fortsetzen**, um die Warnung zu ignorieren und das Skript ausführen zu lassen.

Verwalten potenzieller Würmer

Wenn ActiveShield einen potenziellen Wurm erkennt, können Sie weitere Informationen anzeigen und die E-Mail-Aktivität dann anhalten, wenn Sie nicht möchten, dass sie initialisiert wird:

- Klicken Sie auf **Weitere Informationen**, um die Empfängerliste, die Betreffzeile, den Nachrichtentext und die Beschreibung der zu der entdeckten E-Mail-Nachricht gehörenden verdächtigen Aktivität anzuzeigen.
- Klicken Sie auf **E-Mail anhalten**, um das Senden der verdächtigen E-Mail zu unterbinden und sie aus Ihrer Nachrichtenwarteschlange zu löschen.

Wenn Sie sicher sind, dass die E-Mail-Aktivität vertrauenswürdig ist, klicken Sie auf **Aktuelle Tätigkeit fortsetzen**, um die Warnung zu ignorieren und das Senden der E-Mail zuzulassen.

Verwalten von PUPs

Wenn ActiveShield ein potenziell unerwünschtes Programm (PUP) erkennt und blockiert, können Sie weitere Informationen anzeigen und das Programm dann entfernen, wenn Sie nicht möchten, dass es installiert wird:

- Klicken Sie auf **Weitere Informationen**, um den Namen, den Speicherort und die empfohlene Vorgehensweise für dieses potenziell unerwünschte Programm anzuzeigen.
- Klicken Sie auf **PUP entfernen**, um das Programm zu entfernen, wenn Sie nicht möchten, dass es installiert wird.

  Eine Bestätigungsmeldung wird angezeigt.

  – Wenn Sie (a) das PUP nicht kennen oder (b) das PUP nicht als Bestandteil eines Programmpakets installiert oder keinen Lizenzvertrag für solche Programme akzeptiert haben, klicken Sie auf **OK**, um das Programm mithilfe der Entfernungsmethode von McAfee zu entfernen.

  – Klicken Sie andernfalls auf **Abbrechen**, um den automatischen Entfernungsvorgang zu beenden. Wenn Sie Ihre Meinung später ändern, können Sie das Programm mithilfe des Deinstallationsprogramms des Herstellers manuell entfernen.
- Klicken Sie auf **Aktuelle Tätigkeit fortsetzen**, um die Warnung zu ignorieren und das Programm dieses Mal zu blockieren.

Wenn Sie (a) das PUP kennen oder (b) das PUP möglicherweise als Teil einer Programmgruppe installiert oder einen Lizenzvertrag in Verbindung mit solchen Programmen akzeptiert haben, können Sie die Ausführung dieses Programms zulassen:

- Klicken Sie auf **Dieses PUP als vertrauenswürdig einstufen**, um das Programm in die Liste der vertrauenswürdigen Programme aufzunehmen und seine Ausführung zukünftig immer zuzulassen.

  Genauere Informationen dazu finden Sie unter *Verwalten von vertrauenswürdigen PUPs*.

Verwalten von vertrauenswürdigen PUPs

Programme, die Sie zur Liste der vertrauenswürdigen PUPs hinzufügen, werden von McAfee VirusScan nicht als verdächtig gemeldet.

Wenn ein potenziell unerwünschtes Programm gefunden und zur Liste der vertrauenswürdigen PUPs hinzugefügt wird, können Sie es bei Bedarf jederzeit wieder aus der Liste entfernen.

Wenn die Liste Ihrer vertrauenswürdigen PUPs voll ist, müssen Sie einige Einträge aus der Liste entfernen, bevor Sie einen weiteren Eintrag hinzufügen können.

So entfernen Sie ein Programm aus der Liste der vertrauenswürdigen PUPs:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.
2. Klicken Sie auf **Erweitert** und dann auf die Registerkarte **PUPs**.
3. Klicken Sie auf **Liste der vertrauenswürdigen PUPs bearbeiten**, aktivieren Sie das Kontrollkästchen vor dem Dateinamen, und klicken Sie auf **Entfernen**. Klicken Sie auf **OK**, wenn Sie die gewünschten Einträge entfernt haben.

Manuelles Überprüfen des Computers

Mit der Prüffunktion werden Festplatten, Disketten sowie einzelne Dateien und Ordner nach Viren und anderen Bedrohungen durchsucht. Wird beim Prüfen eine verdächtige Datei gefunden, wird automatisch versucht, die Datei zu bereinigen, sofern es sich dabei nicht um ein potenziell unerwünschtes Programm handelt. Wenn die Datei nicht bereinigt werden kann, können Sie die Datei isolieren oder löschen.

Manuelles Prüfen auf Viren und andere Bedrohungen

So überprüfen Sie Ihren Computer:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Scan**.

Das Dialogfeld **Scan** wird angezeigt (Abbildung 3-8).

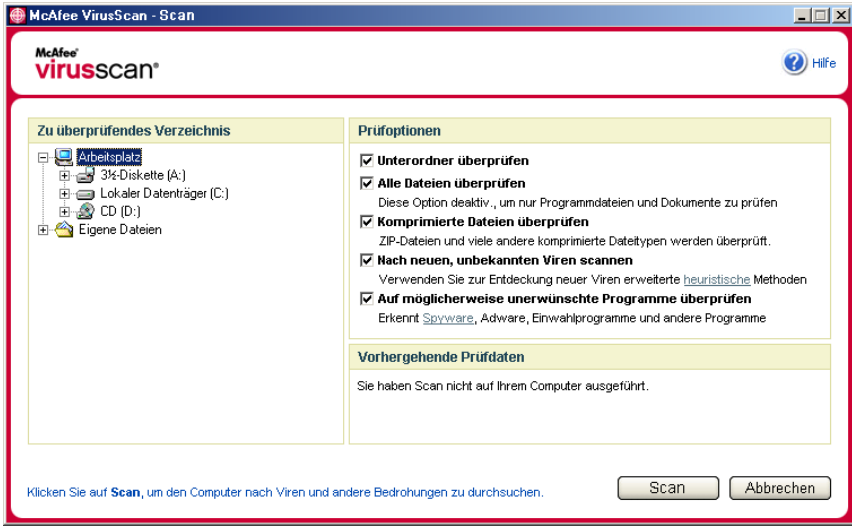

McAfee VirusScan - Scan
McAfee
virusscan
Hilfe
Zu überprüfendes Verzeichnis
Arbeitsplatz
3½-Diskette (A:)
Lokaler Datenträger (C:)
CD (D:)
Eigene Dateien
Prüfoptionen
Unterordner überprüfen
Alle Dateien überprüfen
Diese Option deaktiv., um nur Programmdateien und Dokumente zu prüfen
Komprimierte Dateien überprüfen
ZIP-Dateien und viele andere komprimierte Dateitypen werden überprüft.
Nach neuen, unbekannten Viren scannen
Verwenden Sie zur Entdeckung neuer Viren erweiterte heuristische Methoden
Auf möglicherweise unerwünschte Programme überprüfen
Erkennt Spyware, Adware, Einwahlprogramme und andere Programme
Vorhergehende Prüfdaten
Sie haben Scan nicht auf Ihrem Computer ausgeführt.
Klicken Sie auf Scan, um den Computer nach Viren und andere Bedrohungen zu durchsuchen.
Scan
Abbrechen

Abbildung 3-8. Dialogfeld "Scan"

2 Klicken Sie auf das Laufwerk, den Ordner oder die Datei, die überprüft werden soll.

3 Wählen Sie die gewünschten Prüfoptionen aus. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren Prüfoptionen bereits aktiviert (Abbildung 3-8):

- **Unterordner überprüfen** – Verwenden Sie diese Option, um Dateien in Unterordnern zu überprüfen. Deaktivieren Sie dieses Kontrollkästchen, wenn nur die Dateien überprüft werden sollen, die beim Öffnen eines Ordners oder Laufwerks angezeigt werden.

  Beispiel: Die Dateien in Abbildung 3-9 auf Seite 73 sind die einzigen Dateien, die durchsucht werden, wenn Sie das Kontrollkästchen **Unterordner überprüfen** deaktivieren. Die Ordner und deren Inhalt werden nicht überprüft. Wenn sie möchten, dass auch die Ordner mit den darin enthaltenen Dateien durchsucht werden, müssen Sie das Kontrollkästchen aktiviert lassen.

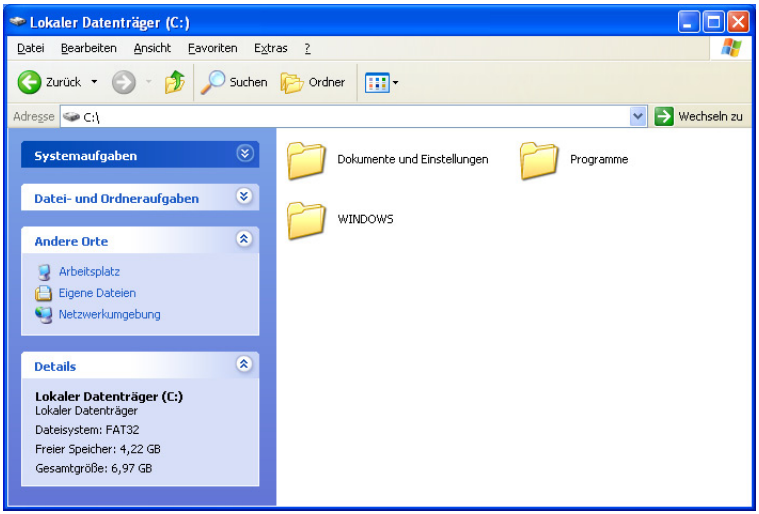


Abbildung 3-9. Inhalt lokaler Datenträger

- **Alle Dateien überprüfen** – Verwenden Sie diese Option, um eine gründliche Überprüfung aller Dateitypen zuzulassen. Deaktivieren Sie dieses Kontrollkästchen, wenn Sie den Prüfvorgang abkürzen und nur Programmdateien und Dokumente überprüfen lassen möchten.
- **Komprimierte Dateien überprüfen** – Verwenden Sie diese Option, um verborgene Dateien in ZIP- und anderen komprimierten Archiven aufzudecken. Deaktivieren Sie dieses Kontrollkästchen, um das Überprüfen von Dateien oder komprimierten Dateien innerhalb von Archiven zu unterbinden.

  Manchmal werden Viren in eine ZIP-Datei eingesetzt und diese ZIP-Datei wiederum in eine weitere ZIP-Datei eingefügt, um Antiviren-Scanner zu umgehen. Wenn die Option **Komprimierte Dateien überprüfen** aktiviert ist, können komprimierte Viren erkannt werden.

- **Nach neuen, unbekannten Viren scannen** – Verwenden Sie diese Option, um die neuesten Viren zu finden, für die es eventuell noch kein "Gegenmittel" gibt. Bei der Option **Nach neuen, unbekannten Viren scannen** werden fortschrittliche heuristische Techniken eingesetzt, um in den Dateien nach Mustern zu suchen, die mit Signaturen bekannter Viren übereinstimmen, oder die zumindest ein Indiz für einen noch unbekannten Virus sein könnten.

  Bei diesem Scanverfahren wird auch nach Dateimerkmalen gesucht, die generell die Möglichkeit ausschließen, dass die entsprechende Datei einen Virus enthält. Damit wird die Wahrscheinlichkeit von Fehlalarmen minimiert. Wenn jedoch mit dem heuristischen Verfahren ein Virus in einer Datei gefunden wird, sollten Sie diese Datei mit derselben Vorsicht behandeln wie eine infizierte Datei.

  Diese Option bietet die gründlichste Überprüfung, ist aber meist zeitaufwendiger als eine normale Überprüfung.

- **Auf möglicherweise unerwünschte Programme überprüfen (empfohlen)** – Verwenden Sie diese Option, um Spyware, Adware und andere Programme zu entdecken, die Ihre privaten Daten sammeln und ohne Ihre Zustimmung weiterleiten.

  HINWEIS
  Lassen Sie alle Optionen aktiviert, um die Überprüfung so gründlich wie möglich durchzuführen. Dadurch dauert die Überprüfung etwas länger, aber jede Datei im ausgewählten Laufwerk oder Ordner wird tatsächlich überprüft. Je größer die Festplatte ist und je mehr Dateien gespeichert sind, desto länger dauert die Überprüfung.

4 Klicken Sie auf **Scan**, um mit dem Überprüfen der Dateien zu beginnen.

Nach Abschluss der Überprüfung wird in einer Zusammenfassung angezeigt, wie viele Dateien überprüft wurden, wie viele Treffer ermittelt wurden, wie viele potenziell unerwünschte Programme gefunden wurden und wie viele infizierte Dateien automatisch bereinigt wurden.

5 Klicken Sie auf **OK**, um die Zusammenfassung zu schließen und die Liste aller entdeckten Dateien im Dialogfeld **Scan** anzuzeigen (Abbildung 3-10).

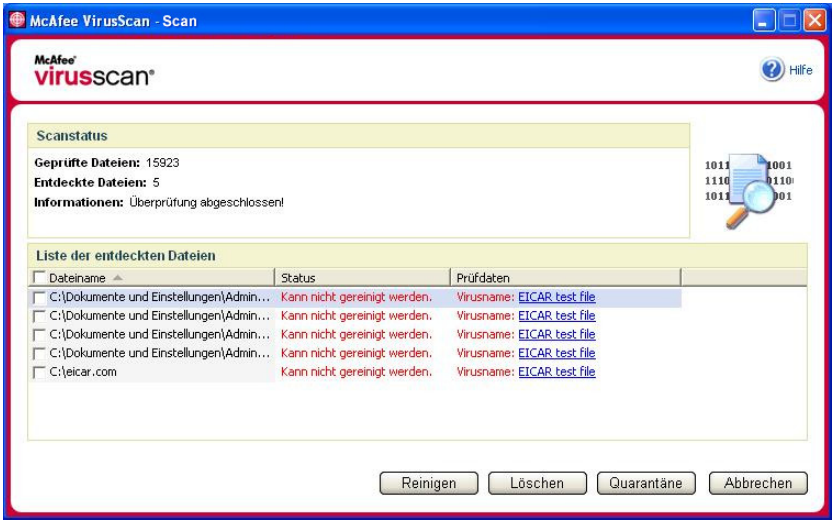


Abbildung 3-10. Prüfergebnisse

HINWEIS
Unter **Geprüfte Dateien** zählt Scan komprimierte Dateien (z. B. ZIP, CAB) jeweils als eine Datei. Die Anzahl der durchsuchten Dateien kann auch variieren, wenn Sie seit der letzten Überprüfung Ihre temporären Internetdateien gelöscht haben.

6 Wenn bei der Überprüfung keine Viren oder andere Bedrohungen gefunden wurden, klicken Sie auf **Zurück**, um ein anderes Laufwerk oder einen anderen Ordner zum Überprüfen auszuwählen, oder klicken Sie auf **Schließen**, um das Dialogfeld zu schließen. Andernfalls finden Sie unter *Grundlegendes zu Bedrohungserkennungen* auf Seite 78 weitere Informationen.

Prüfen per Windows Explorer

VirusScan stellt ein Kontextmenü zur Verfügung, mit dem im Windows Explorer ausgewählte Dateien, Ordner oder Laufwerke auf Viren und andere Bedrohungen überprüft werden können.

So überprüfen Sie Dateien im Windows Explorer:

1 Öffnen Sie Windows Explorer.

2 Klicken Sie mit der rechten Maustaste auf das Laufwerk, den Ordner oder die Datei, die überprüft werden soll, und klicken Sie dann auf **Scan**.

Das Dialogfeld **Scan** wird angezeigt, und die Überprüfung der Dateien wird gestartet. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren **Prüfoptionen** aktiviert (Abbildung 3-8 auf Seite 72).

Prüfen per Microsoft Outlook

VirusScan stellt ein Symbol auf der Symbolleiste bereit, mit dem ausgewählte Nachrichtenspeicher und deren zugehörige Unterordner, Postfachordner oder E-Mail-Nachrichten mit Anlagen in Microsoft Outlook 97 (oder höher) auf Viren und andere Bedrohungen überprüft werden können.

So überprüfen Sie E-Mails in Microsoft Outlook:

1 Öffnen Sie Microsoft Outlook.

2 Klicken Sie auf den Nachrichtenspeicher, den Ordner oder die E-Mail-Nachricht mit Anlage, den oder die Sie überprüfen möchten, und klicken Sie dann in der Symbolleiste auf das E-Mail-Scan-Symbol .

Der E-Mail-Scanner wird geöffnet und beginnt mit der Überprüfung der Dateien. Standardmäßig sind für eine möglichst gründliche Überprüfung alle verfügbaren **Prüfoptionen** aktiviert (Abbildung 3-8 auf Seite 72).

Automatisches Überprüfen auf Viren und andere Bedrohungen

Obwohl VirusScan Dateien überprüft, wenn Sie oder Ihr Computer darauf zugreifen, können Sie im Windows-Taskplaner die automatische Überprüfung planen, um den Computer in festgelegten Intervallen gründlich nach Viren und anderen Bedrohungen zu durchsuchen.

So planen Sie einen Scanvorgang:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

Das Dialogfeld **VirusScan - Optionen** wird geöffnet.

2 Klicken Sie auf die Registerkarte **Geplanter Scanvorgang** (Abbildung 3-11).

Abbildung 3-11. Optionen für geplante Scanvorgänge

3 Aktivieren Sie das Kontrollkästchen **Computer zu einem festgelegten Zeitpunkt überprüfen**, um das automatische Scannen zu aktivieren.

4 So planen Sie einen automatischen Scanvorgang:

- Wenn Sie den standardmäßigen Zeitplan (freitags um 20 Uhr) akzeptieren möchten, klicken Sie auf **OK**.
- So bearbeiten Sie den Zeitplan:

  a. Klicken Sie auf **Bearbeiten**.

  b. Legen Sie in der Liste **Geplante Tasks** fest, wie oft der Computer auf Viren überprüft werden soll, und wählen Sie dann weitere Optionen in dem darunter liegenden dynamischen Bereich aus:

  Täglich – Geben Sie die Anzahl der Tage zwischen den Scanvorgängen ein.

  Wöchentlich (Standardeinstellung) – Geben Sie die Anzahl der Wochen zwischen den Scanvorgängen und die Wochentage an, an denen die Scans ausgeführt werden sollen.

Monatlich – Geben Sie den Tag an, an dem der Scanvorgang ausgeführt werden soll. Klicken Sie auf **Monate auswählen**, um die Monate festzulegen, in denen gescannt werden soll, und klicken Sie dann auf **OK**.

Einmal – Geben Sie ein Datum für den Scanvorgang an.

HINWEIS
Die folgenden Optionen im Windows-Taskplaner werden nicht unterstützt:
Beim Systemstart, **Im Leerlauf** und **Mehrfache Zeitpläne anzeigen**. Der letzte unterstützte Zeitplan bleibt so lange aktiv, bis Sie eine der gültigen Optionen auswählen.

c. Wählen Sie im Feld **Startzeit** die Uhrzeit aus, zu der der Computer überprüft werden soll.

d. Wenn Sie erweiterte Optionen auswählen möchten, klicken Sie auf **Erweitert**.

Das Dialogfeld **Erweiterte Zeitplanoptionen** wird angezeigt.

i. Geben Sie Anfangsdatum, Enddatum, Dauer und Endzeitpunkt ein, und geben Sie an, ob der Scanvorgang zur festgelegten Zeit beendet werden soll, wenn die Überprüfung noch ausgeführt wird.

ii. Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen. Klicken Sie andernfalls auf **Abbrechen**.

5 Klicken Sie auf **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen. Klicken Sie andernfalls auf **Abbrechen**.

6 Wenn Sie den standardmäßigen Zeitplan wiederherstellen möchten, klicken Sie auf **Als Standard festlegen**. Klicken Sie andernfalls auf **OK**.

Grundlegendes zu Bedrohungserkennungen

Bei den meisten Viren, Trojanern und Würmern versucht Scan automatisch, die Datei zu bereinigen. Anschließend können Sie angeben, wie mit als infiziert erkannten Dateien verfahren werden soll und ob sie zu Forschungszwecken an die McAfee AVERT-Labore übermittelt werden sollen. Wenn die Scan-Funktion ein potenziell unerwünschtes Programm findet, können Sie versuchen, es manuell zu bereinigen, zu isolieren oder zu löschen (Einsenden an AVERT ist nicht möglich).

So gehen Sie bei einem Virus oder potenziell unerwünschten Programm vor:

1 Wenn eine Datei in der **Liste der erkannten Dateien** angezeigt wird, aktivieren Sie das Kontrollkästchen vor der Datei, um sie auszuwählen.

> **HINWEIS**
> Wenn in der Liste mehrere Dateien angezeigt werden, können Sie das Kontrollkästchen vor der Liste **Dateiname** aktivieren, um denselben Vorgang für alle Dateien durchzuführen. Sie können auch auf den Dateinamen in der Liste **Prüfdaten** klicken, um detaillierte Informationen aus der Virenbibliothek anzuzeigen.

2 Wenn es sich bei der Datei um ein potenziell unerwünschtes Programm handelt, können Sie auf **Reinigen** klicken, um zu versuchen, die Datei zu bereinigen.

3 Wenn Scan die Datei nicht bereinigen kann, klicken Sie auf **Quarantäne**, um verdächtige Dateien zu verschlüsseln und im Quarantäneverzeichnis vorübergehend zu isolieren, bis eine angemessene Maßnahme ergriffen werden kann. (Nähere Informationen dazu finden Sie unter *Verwalten von isolierten Dateien* auf Seite 80.)

4 Wenn Scan die Datei nicht bereinigen oder isolieren kann, können Sie einen der folgenden Schritte ausführen:

- Klicken Sie auf **Löschen**, um die Datei zu entfernen.
- Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, ohne weitere Aktionen durchzuführen.

Wenn Scan die erkannte Datei weder bereinigen noch löschen kann, finden Sie weitere Informationen in der Virenbibliothek unter http://de.mcafee.com/virusInfo/. Dort finden Sie Anweisungen zum manuellen Löschen der Datei.

Wenn die erkannte Datei verhindert, dass Sie eine Internetverbindung herstellen oder Ihren Computer generell nicht mehr verwenden können, versuchen Sie, den Computer mit einer Rettungsdiskette neu zu starten. In vielen Fällen kann ein infizierter Computer mithilfe der Rettungsdiskette gestartet werden, wenn dies anders nicht mehr möglich ist. Nähere Informationen dazu finden Sie unter *Erstellen einer Rettungsdiskette* auf Seite 82.

Weitere Hilfe erhalten Sie vom McAfee-Kundendienst unter http://www.mcafeehilfe.com/.

Verwalten von isolierten Dateien

Mithilfe der Quarantäne-Funktion können Sie verdächtige Dateien verschlüsseln und in einem Quarantäneverzeichnis vorübergehend isolieren, bis eine angemessene Maßnahme ergriffen werden kann. Nach dem Bereinigen kann eine isolierte Datei an ihrem ursprünglichen Speicherort wiederhergestellt werden.

So verwalten Sie eine isolierte Datei:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Dateien unter Quarantäne verwalten**.

Eine Liste mit isolierten Dateien wird angezeigt (Abbildung 3-12).

Abbildung 3-12. Dialogfeld "Dateien unter Quarantäne verwalten"

2 Aktivieren Sie das Kontrollkästchen neben den Dateien, die bereinigt werden sollen.

HINWEIS
Wenn in der Liste mehrere Dateien angezeigt werden, können Sie das Kontrollkästchen vor der Liste **Dateiname** aktivieren, um denselben Vorgang für alle Dateien durchzuführen. Sie können auch auf den Virusnamen in der Liste **Status** klicken, um detaillierte Informationen aus der Virenbibliothek anzuzeigen.

Oder Sie klicken auf **Hinzufügen**, wählen eine verdächtige Datei aus, die der Quarantäneliste hinzugefügt werden soll, klicken dann auf **Öffnen**, und wählen die Datei in der Quarantäneliste aus.

3 Klicken Sie auf **Reinigen**.

4 Wenn die Datei bereinigt ist, klicken Sie auf **Wiederherstellen**, um die Datei wieder an ihren ursprünglichen Speicherort zu verschieben.

5 Wenn VirusScan den Virus nicht bereinigen kann, klicken Sie auf **Löschen**, um die Datei zu entfernen.

6 Wenn VirusScan die Datei nicht bereinigen oder löschen kann und es sich nicht um ein potenziell unerwünschtes Programm handelt, können Sie die Datei zu Forschungszwecken an das McAfee AntiVirus Emergency Response Team (AVERT™) übermitteln:

a Aktualisieren Sie Ihre Virussignaturdateien spätestens alle zwei Wochen.

b Überprüfen Sie Ihr Abonnement.

c Wählen Sie die Datei aus, und klicken Sie auf **Senden**, um die Datei an AVERT zu übermitteln.

VirusScan sendet die isolierte Datei als Anlage in einer E-Mail-Nachricht, die Ihre E-Mail-Adresse, Ihr Land, die Softwareversion, das Betriebssystem sowie den ursprünglichen Namen und Speicherort der Datei enthält. Das maximale Sendevolumen für die Übermittlung von Dateien beträgt 1,5 MB pro Tag.

7 Klicken Sie auf **Abbrechen**, um das Dialogfeld zu schließen, ohne weitere Aktionen durchzuführen.

Erstellen einer Rettungsdiskette

Das Programm zum Erstellen einer Rettungsdiskette ist ein Dienstprogramm, das eine startfähige Diskette erstellt, mit der Sie einen nicht mehr startfähigen infizierten Computer starten und auf Viren überprüfen können.

HINWEIS
Sie müssen mit dem Internet verbunden sein, um die Imagedatei für die Rettungsdiskette herunterladen zu können. Das Programm zum Erstellen einer Rettungsdiskette ist nur für Computer mit FAT-Partitionen (FAT 16 und FAT 32) verfügbar. Bei NTFS-Partitionen ist es nicht erforderlich.

So erstellen Sie eine Rettungsdiskette:

1. Legen Sie eine nicht infizierte Diskette in das Laufwerk A eines nicht infizierten Computers ein. Sie können Scan verwenden, wenn Sie sicherstellen möchten, dass Computer und Diskette virenfrei sind. (Nähere Informationen dazu finden Sie unter *Manuelles Prüfen auf Viren und andere Bedrohungen* auf Seite 71.)

2. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Rettungsdiskette erstellen**.

   Das Dialogfeld **Rettungsdiskette erstellen** wird angezeigt (Abbildung 3-13).

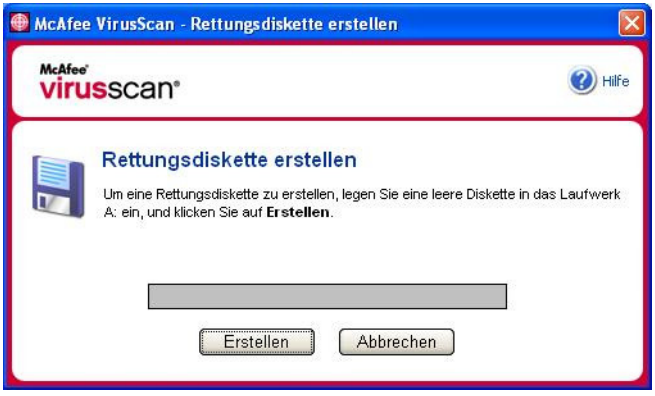

McAfee VirusScan - Rettungsdiskette erstellen
McAfee
virusscan
Hilfe
Rettungsdiskette erstellen
Um eine Rettungsdiskette zu erstellen, legen Sie eine leere Diskette in das Laufwerk A: ein, und klicken Sie auf Erstellen.
Erstellen
Abbrechen

Abbildung 3-13. Dialogfeld "Rettungsdiskette erstellen"

3 Klicken Sie auf **Erstellen**, um die Rettungsdiskette zu erstellen.

Wenn Sie zum ersten Mal eine Rettungsdiskette erstellen, werden Sie in einer Meldung darüber informiert, dass die Imagedatei für die Rettungsdiskette heruntergeladen werden muss. Klicken Sie auf **OK**, um die Komponente jetzt herunterzuladen, oder auf **Abbrechen**, um sie zu einem späteren Zeitpunkt herunterzuladen.

Es wird eine Warnung angezeigt, die Sie darüber informiert, dass alle Inhalte auf der Diskette gelöscht werden.

4 Klicken Sie auf **Ja**, um mit dem Erstellen der Rettungsdiskette fortzufahren.

Der Status des Erstellungsvorgangs wird im Dialogfeld **Rettungsdiskette erstellen** angezeigt.

5 Wenn die Meldung "Rettungsdiskette erstellt" angezeigt wird, klicken Sie auf **OK**, und schließen Sie dann das Dialogfeld **Rettungsdiskette erstellen**.

6 Entnehmen Sie die Rettungsdiskette aus dem Laufwerk, versehen Sie sie mit einem Schreibschutz, und bewahren Sie sie an einem sicheren Ort auf.

Einrichten des Schreibschutzes für eine Rettungsdiskette

So richten Sie den Schreibschutz für eine Rettungsdiskette ein:

1 Drehen Sie die Diskette mit der Beschriftungsseite nach unten (die runde Metallplatte muss sichtbar sein).

2 Suchen Sie den Riegel für den Schreibschutz. Verschieben Sie den Riegel so, dass die Öffnung sichtbar ist.

Verwenden einer Rettungsdiskette

So verwenden Sie eine Rettungsdiskette:

1 Schalten Sie den infizierten Computer aus.

2 Legen Sie die Rettungsdiskette in das Diskettenlaufwerk ein.

3 Schalten Sie den Computer wieder ein.

Es wird ein graues Fenster mit verschiedenen Optionen angezeigt.

4 Wählen Sie die gewünschte Option aus, indem Sie die entsprechende Funktionstaste (F2, F3 usw.) drücken.

HINWEIS
Wenn Sie keine dieser Tasten drücken, wird das Rettungsdiskettenprogramm nach 60 Sekunden automatisch gestartet.

Aktualisieren einer Rettungsdiskette

Es empfiehlt sich, Ihre Rettungsdiskette regelmäßig zu aktualisieren. Folgen Sie dazu den Anweisungen zum Erstellen einer neuen Rettungsdiskette.

Automatisches Melden von Viren

Informationen zu Viren können anonym an die World Virus Map gesendet werden. Das Angebot, diese kostenlose, sichere Funktion zu nutzen, nehmen Sie entweder automatisch während der Installation von VirusScan (im Dialogfeld **Informationen an Virus Map weiterleiten**) an, oder Sie können es jederzeit im Dialogfeld **VirusScan - Optionen** auf der Registerkarte **Virus Map melden** akzeptieren.

Melden von Vireninformationen an die World Virus Map

So melden Sie Vireninformationen automatisch an die World Virus Map:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **Optionen**.

   Das Dialogfeld **VirusScan - Optionen** wird geöffnet.

2. Klicken Sie auf die Registerkarte **Virus Map melden** (Abbildung 3-14).

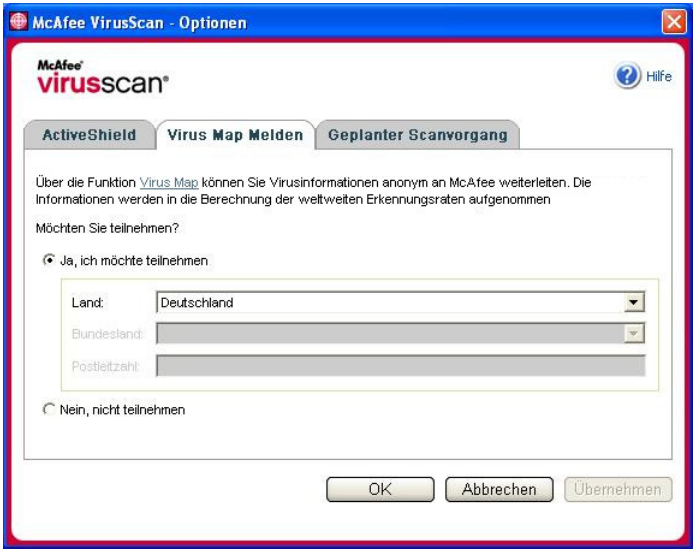


Abbildung 3-14. Optionen für die Weiterleitung von Informationen an Virus Map

3 Akzeptieren Sie die Standardoption **Ja, ich möchte teilnehmen**, wenn Sie Ihre Informationen anonym an McAfee senden möchten, wo sie bei der Ermittlung globaler Erkennungsraten in der World Virus Map berücksichtigt werden. Wählen Sie andernfalls **Nein, nicht teilnehmen**. Ihre Informationen werden in diesem Falle nicht gesendet.

4 Wenn Sie in den USA leben, wählen Sie den Bundesstaat aus, und geben Sie die Postleitzahl (Zip-Code) für den Standort Ihres Computers ein. Wenn Sie nicht in den USA leben, versucht VirusScan automatisch das Land auszuwählen, in dem sich Ihr Computer befindet.

5 Klicken Sie auf **OK**.

Anzeigen der World Virus Map

Auch wenn Sie keine Informationen an die World Virus Map senden, können Sie die aktuellsten globalen Erkennungsraten über das McAfee-Symbol auf der Windows-Taskleiste anzeigen.

So zeigen Sie die World Virus Map an:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **VirusScan**, und klicken Sie dann auf **World Virus Map**.

  Die Webseite mit der **World Virus Map** wird angezeigt (Abbildung 3-15).

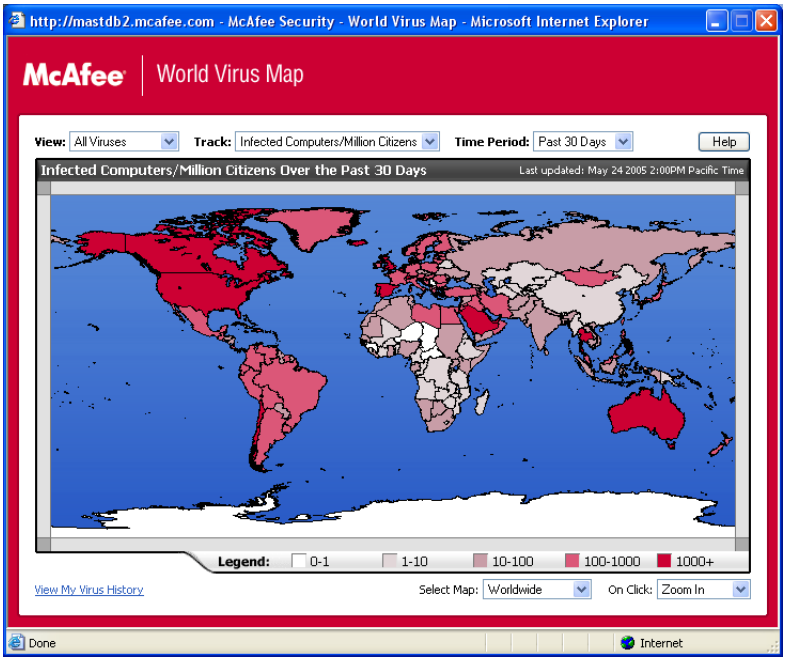

http://mastdb2.mcafee.com - McAfee Security - World Virus Map - Microsoft Internet Explorer
McAfee
World Virus Map
View: All Viruses
Track: Infected Computers/Million Citizens
Time Period: Past 30 Days
Help
Infected Computers/Million Citizens Over the Past 30 Days
Last updated: May 24 2005 2:00PM Pacific Time
Legend: 0-1 1-10 10-100 100-1000 1000+
View My Virus History
Select Map: Worldwide
On Click: Zoom In
Done
Internet

Abbildung 3-15. World Virus Map

Standardmäßig zeigt die World Virus Map die Anzahl der Computer an, die weltweit in den letzten 30 Tagen entdeckt wurden. Außerdem wird angegeben, wann die gemeldeten Daten zuletzt aktualisiert wurden. Sie können die Ansicht der World Virus Map so ändern, dass die Anzahl der entdeckten Dateien angezeigt wird, oder den Zeitraum bearbeiten, um nur die Ergebnisse der letzten sieben Tage oder der letzten 24 Stunden darzustellen.

Im Prüfbereich finden Sie eine Auflistung der gesamten durchsuchten Dateien sowie der entdeckten Dateien und Computer, die seit dem angegebenen Datum gemeldet wurden.

Aktualisieren von VirusScan

Wenn Ihr Computer mit dem Internet verbunden ist, sucht VirusScan automatisch alle vier Stunden nach Updates und lädt dann automatisch einmal pro Woche Updates von Virusdefinitionen herunter und installiert diese, ohne Sie bei der Arbeit zu unterbrechen.

Virusdefinitionsdateien sind maximal 100 KB groß und beeinträchtigen die Systemleistung während des Downloads folglich nur geringfügig.

Ist ein Produktupdate verfügbar oder hat ein Virenausbruch stattgefunden, wird eine entsprechende Warnmeldung angezeigt. Sie können dann VirusScan aktualisieren, um die Verbreitung des Virus zu verhindern.

Automatisches Prüfen auf Updates

McAfee SecurityCenter ist so konfiguriert, dass bei einer bestehenden Internetverbindung alle vier Stunden automatisch nach Updates für Ihre gesamten McAfee-Dienste gesucht wird, und Sie durch Warnmeldungen und akustische Signale benachrichtigt werden. Standardmäßig werden verfügbare Updates automatisch von SecurityCenter heruntergeladen und installiert.

HINWEIS
In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Vergewissern Sie sich, dass Sie Ihre Arbeit gespeichert und alle Programme geschlossen haben, bevor Sie den Neustart durchführen.

Manuelles Prüfen auf Updates

Zusätzlich zur automatischen Suche nach Updates, die bei einer bestehenden Internetverbindung alle vier Stunden durchgeführt wird, können Sie auch jederzeit manuell nach Updates suchen.

So suchen Sie manuell nach VirusScan-Updates:

1. Stellen Sie sicher, dass Ihr Computer mit dem Internet verbunden ist.
2. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, und klicken Sie dann auf **Aktualisieren**.

   Das Dialogfeld **SecurityCenter-Updates** wird geöffnet.
3. Klicken Sie auf **Jetzt prüfen**.

   Wenn ein Update vorhanden ist, wird das Dialogfeld **VirusScan - Updates** geöffnet (Abbildung 3-16 auf Seite 88). Klicken Sie auf **Aktualisieren**, um den Vorgang fortzusetzen.

Wenn keine Updates verfügbar sind, werden Sie in einem Dialogfeld darüber informiert, dass VirusScan auf dem neuesten Stand ist. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

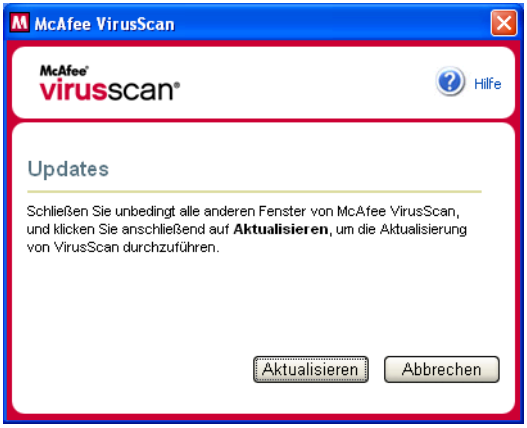


Abbildung 3-16. Dialogfeld "Updates"

4 Melden Sie sich bei der Website an, wenn Sie dazu aufgefordert werden. Das Update wird automatisch vom **Update-Assistenten** installiert.

5 Klicken Sie nach Abschluss der Update-Installation auf **Fertig stellen**.

HINWEIS
In einigen Fällen werden Sie aufgefordert, den Computer neu zu starten, um den Installationsvorgang für das Update abzuschließen. Vergewissern Sie sich, dass Sie Ihre Arbeit gespeichert und alle Programme geschlossen haben, bevor Sie den Neustart durchführen.

McAfee Personal Firewall Plus 4

Willkommen bei McAfee Personal Firewall Plus.

McAfee Personal Firewall Plus bietet fortschrittlichen Schutz für Ihren Computer und Ihre persönlichen Daten. Personal Firewall errichtet eine Barriere zwischen Ihrem Computer und dem Internet. Dabei wird der Internetverkehr im Hintergrund auf verdächtige Aktivitäten hin überwacht.

Das Programm umfasst folgende Funktionen:

- Abwehr von potenziellen Hacker-Angriffen
- Ergänzung zu Antivirensoftware
- Überwachung von Internet- und Netzwerkaktivitäten
- Warnungen bei potenziell feindlichen Ereignissen
- Detaillierte Informationen zu verdächtigem Internetverkehr
- Integration der Funktionalität von HackerWatch.org. Dazu gehören: Das Melden von Ereignissen, Tools, die sich selbst testen, und die Fähigkeit, gemeldete Ereignisse per E-Mail an andere Online-Behörden zu senden.
- Detaillierte Funktionen zur Nachverfolgung und Ereignisrecherche

Neue Funktionen

- **Verbesserte Spiele-Unterstützung**
  McAfee Personal Firewall Plus schützt Ihren Computer vor Eindringungsversuchen und verdächtigen Aktivitäten, während Sie Spiele im Vollbildmodus spielen, wobei die entsprechenden Warnungen aber auch ausgeblendet werden können. Erst nachdem Sie das Spiel beendet haben, werden rote Warnmeldungen angezeigt.

- **Verbesserte Zugriffsverwaltung**
  Mit McAfee Personal Firewall Plus können Sie Anwendungen dynamisch einen vorübergehenden Zugriff auf das Internet gewähren. Der Zugriff ist auf den Zeitraum zwischen Starten und Beenden der Anwendung beschränkt. Entdeckt Personal Firewall ein unbekanntes Programm, das versucht, mit dem Internet zu kommunizieren, erhalten Sie in einer roten Warnmeldung die Möglichkeit, der Anwendung vorübergehend Zugriff auf das Internet zu gewähren.

- **Erweiterte Sicherheitskontrolle**
  Mithilfe der Sperrfunktion **Verbindung trennen** in McAfee Personal Firewall Plus können Sie den gesamten eingehenden und ausgehenden Internetverkehr zwischen Computer und Internet sofort sperren. Sie können den Sperrmodus an drei verschiedenen Stellen in Personal Firewall aktivieren und deaktivieren.

- **Verbesserte Optionen für die Wiederherstellung**
  Sie können die Optionen zurücksetzen, um die Standardeinstellungen für Personal Firewall automatisch wiederherzustellen. Wenn sich Personal Firewall nicht so verhält, wie Sie es wünschen, haben Sie die Möglichkeit, Ihre aktuellen Einstellungen rückgängig zu machen und die Standardeinstellungen des Produkts wiederherzustellen.

- **Schutz für die Internetverbindung**
  Damit ein Benutzer nicht versehentlich die Internetverbindung deaktiviert, wird bei einer blauen Warnung die Option zum Sperren der Internetadresse nicht angezeigt, wenn Personal Firewall erkannt hat, dass die Internetverbindung von einem DHCP- oder DNS-Server hergestellt wurde. Wenn der eingehende Datenverkehr nicht von einem DHCP- oder DNS-Server stammt, wird die Option angezeigt.

- **Verbesserte HackerWatch.org-Integration**
  Das Melden potenzieller Hacker ist einfacher denn je. McAfee Personal Firewall Plus verbessert die Funktionalität von HackerWatch.org (dazu gehört u. a. die Übermittlung potenziell bösartiger Ereignisse an die Datenbank).

- **Erweiterter intelligenter Umgang mit Anwendungen**
  Wenn eine Anwendung Internetzugriff anfordert, prüft Personal Firewall zuerst, ob die Anwendung als vertrauenswürdig oder bösartig bekannt ist. Gilt die Anwendung als vertrauenswürdig, gewährt Personal Firewall ihr automatisch den Zugriff auf das Internet, ohne dass Sie etwas dazu tun müssen.

- **Fortschrittliche Erkennung von Trojanern**
  Beim Verwalten der Verbindungen von Anwendungen nutzt McAfee Personal Firewall Plus eine erweiterte Datenbank, um mehr potenziell bösartige Anwendungen (z. B. Trojaner) erkennen und blockieren und somit daran hindern zu können, auf das Internet zuzugreifen und möglicherweise Ihre persönlichen Daten weiterzugeben.

- **Verbesserte visuelle Nachverfolgung**
  Visual Trace bietet leicht verständliche grafische Darstellungen, in denen die Quelle der feindlichen Angriffe und des weltweiten Datenverkehrs einschließlich detaillierter Kontakt- bzw. Benutzerinformationen zu den Quell-IP-Adressen angezeigt werden.

- **Verbesserte Benutzerfreundlichkeit**
  McAfee Personal Firewall Plus enthält einen Setup-Assistenten und ein User Tutorial, um Benutzer beim Einrichten und Verwenden der Firewall zu unterstützen. Obwohl das Produkt zum eigenständigen Arbeiten ausgelegt ist, stellt McAfee den Benutzern zahlreiche Ressourcen zur Verfügung, um ihnen das Verständnis der Firewall zu erleichtern und deren Nutzen zu verdeutlichen.

- **Erweiterte Eindringungserkennung**
  Das Eindringungserkennungssystem (Intrusion Detection System, IDS) von Personal Firewall erkennt gängige Angriffstypen sowie andere verdächtige Aktivitäten. Die Eindringungserkennung prüft jedes Datenpaket auf verdächtige Datenübertragungen oder Übertragungsmethoden und vermerkt diese im Ereignisprotokoll.

- **Verbesserte Datenverkehrsanalyse**
  Mit McAfee Personal Firewall Plus können Benutzer sowohl eingehende als auch ausgehende Daten Ihres Computers anzeigen. Darüber hinaus können Anwendungsverbindungen sowie Anwendungen angezeigt werden, die aktiv nach offenen Verbindungen suchen. Hierdurch wird es Benutzern ermöglicht, Anwendungen zu erkennen, die möglicherweise ein Risiko darstellen, und entsprechende Gegenmaßnahmen ergreifen.

Deinstallieren anderer Firewalls

Bevor Sie McAfee Personal Firewall Plus installieren, müssen Sie alle anderen Firewall-Programme auf Ihrem Computer deinstallieren. Folgen Sie dazu den Deinstallationsanweisungen des jeweiligen Firewall-Programms.

HINWEIS
Wenn Sie Windows XP verwenden, müssen Sie die integrierte Firewall vor der Installation von McAfee Personal Firewall Plus nicht deaktivieren. Es wird jedoch empfohlen, die integrierte Firewall zu deaktivieren. Andernfalls werden keine Ereignisse im Protokoll für eingehende Ereignisse von McAfee Personal Firewall Plus eingetragen.

Festlegen der Standard-Firewall

McAfee Personal Firewall kann Berechtigungen und Datenverkehr für Internetanwendungen auf Ihrem Computer auch dann verwalten, wenn auf Ihrem Computer die Windows-Firewall als ausgeführt erkannt wird.

Bei der Installation deaktiviert McAfee Personal Firewall automatisch die Windows-Firewall und legt sich selbst als standardmäßige Firewall fest. Alle Firewall-Funktionen und -Meldungen stammen dann ausschließlich von McAfee Personal Firewall. Wenn Sie später die Windows-Firewall über das Windows-Sicherheitscenter oder die Windows-Systemsteuerung aktivieren, so dass auf Ihrem Computer beide Firewalls ausgeführt werden, kann die Protokollfunktion in McAfee Firewall teilweise verloren gehen, während Status- und Warnmeldungen möglicherweise doppelt angezeigt werden.

HINWEIS

Wenn beide Firewalls aktiviert sind, zeigt McAfee Personal Firewall auf der Registerkarte **Eingehende Ereignisse** nicht alle blockierten IP-Adressen an. Die Windows-Firewall fängt die meisten dieser Ereignisse ab und blockiert sie, wodurch ihre Erkennung und Protokollierung durch McAfee Personal Firewall unterbunden wird. McAfee Personal Firewall kann jedoch anhand anderer Sicherheitsfaktoren weiteren Datenverkehr blockieren, der dann auch protokolliert wird.

Das Protokollieren ist in der Windows-Firewall standardmäßig deaktiviert. Wenn Sie jedoch beide Firewalls verwenden möchten, können Sie die Protokollfunktion der Windows-Firewall aktivieren. Das Standardprotokoll der Windows-Firewall ist C:\Windows\pfirewall.log.

Um sicherzustellen, dass Ihr Computer durch mindestens eine Firewall geschützt ist, wird die Windows-Firewall beim Deinstallieren von McAfee Personal Firewall automatisch wieder aktiviert.

Wenn Sie McAfee Personal Firewall deaktivieren oder die Sicherheitseinstellung des Programms auf **Offen** setzen, ohne die Windows-Firewall manuell zu aktivieren, wird sämtlicher Firewall-Schutz (mit Ausnahme der zuvor bereits blockierten Anwendungen) entfernt.

Festlegen der Sicherheitsstufe

Anhand von Sicherheitsoptionen können Sie festlegen, wie Personal Firewall reagieren soll, wenn unerwünschter Datenverkehr erkannt wird. Standardmäßig ist die Sicherheitsstufe **Standard** aktiviert. Wenn eine Anwendung in der Sicherheitsstufe **Standard** Zugriff auf das Internet anfordert und Sie der Anforderung nachkommen, gewähren Sie der Anwendung damit Vollzugriff. Der Vollzugriff erlaubt der Anwendung das Senden und Empfangen unangeforderter Daten auf systemfremden Ports.

So konfigurieren Sie Sicherheitseinstellungen:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Optionen** aus.

2 Klicken Sie auf das Symbol **Sicherheitseinstellungen**.

3 Stellen Sie mit dem Schieberegler die gewünschte Sicherheitsstufe ein.

Die Sicherheitsstufen reichen von **Verbindung schließen** bis **Offen**:

- **Verbindung schließen** – Alle Internetverbindungen Ihres Computers werden geschlossen. Mit dieser Einstellung können Sie Anschlüsse blockieren, die Sie auf der Seite **Systemdienste** als offen konfiguriert haben.
- **Eingeschränkte Sicherheit** – Wenn eine Anwendung einen bestimmten Typ von Internetzugriff erfordert (z. B. "Nur ausgehender Zugriff"), können Sie die Internetverbindung für diese Anwendung zulassen oder blockieren. Wenn eine Anwendung später Vollzugriff anfordert, können Sie den Vollzugriff entweder gewähren oder auf den ausgehenden Datenverkehr einschränken.
- **Standardsicherheit (empfohlen)** – Wenn eine Anwendung Internetzugriff anfordert und Sie der Anforderung nachkommen, erhält die Anwendung damit Vollzugriff für eingehenden und ausgehenden Datenverkehr.
- **Vertrauenswürdige Sicherheit** – Allen Anwendungen wird bei ihrem ersten Versuch, auf das Internet zuzugreifen, automatisch vertraut. Sie können Personal Firewall jedoch so konfigurieren, dass Sie durch Warnungen über neue Anwendungen auf Ihrem Computer informiert werden. Verwenden Sie diese Einstellung, wenn Sie bemerken, dass bestimmte Spiele oder Streaming Media nicht funktionieren.
- **Offen (Kein Filter)** – Ihre Firewall ist deaktiviert. Diese Einstellung lässt den gesamten Datenverkehr durch Personal Firewall ohne Filterung passieren.

HINWEIS
Zuvor blockierte Anwendungen werden auch weiterhin blockiert, wenn die Sicherheitseinstellung der Firewall auf **Offen (Kein Filter)** oder **Verbindung schließen** gesetzt ist. Wenn dies nicht erwünscht ist, können Sie entweder die Berechtigungen der Anwendung in **Vollzugriff** ändern oder die Berechtigungsregel **Diese Anwendung blockieren** aus der Liste **Internetanwendungen** löschen.

4 Auswählen zusätzlicher Sicherheitseinstellungen:

HINWEIS
Wenn auf Ihrem Computer Windows XP ausgeführt wird und mehrere XP-Benutzer hinzugefügt wurden, stehen diese Optionen nur dann zur Verfügung, wenn Sie auf Ihrem Computer als Administrator angemeldet sind.

- **Ereignisse der Eindringungserkennung im Protokoll der eingehenden Ereignisse aufzeichnen** – Wenn Sie diese Option auswählen, werden die von IDS erkannten Ereignisse im Protokoll eingehender Ereignisse angezeigt. Das Eindringungserkennungssystem erkennt gängige Angriffstypen sowie andere verdächtige Aktivitäten. Die Eindringungserkennung überwacht jedes eingehende und ausgehende Datenpaket auf verdächtige Datenübertragungen oder Übertragungsmethoden. Die Pakete werden mit einer Signaturdatenbank verglichen und diejenigen automatisch verworfen, die vom "schuldigen" Computer kommen.

  IDS sucht nach bestimmten Mustern im Datenverkehr, die von Angreifern verwendet werden. Jedes von Ihrem Computer empfangene Datenpaket wird von IDS überprüft, um angriffsverdächtigen oder -bekannten Datenverkehr zu erkennen. Wenn Personal Firewall beispielsweise ICMP-Pakete erkennt, prüft es diese Pakete auf verdächtige Verkehrsmuster, indem es den ICMP-Datenverkehr mit den Mustern bekannter Angriffe vergleicht.

- **ICMP-Pinganforderungen** – ICMP-Datenverkehr wird hauptsächlich für Nachverfolgungen und Pingsignale verwendet. Pingsignale werden häufig zum Durchführen von kurzen Tests verwendet, bevor versucht wird, eine Kommunikation zu initiieren. Wenn Sie ein Peer-to-Peer-Dateifreigabeprogramm verwenden oder verwendet haben, ist es möglich, dass Sie eine große Anzahl von Pingsignalen erhalten. Wenn Sie diese Option auswählen, lässt Personal Firewall alle Pinganforderungen zu, ohne die Pingsignale im Protokoll für eingehende Ereignisse zu vermerken. Wenn Sie die Option nicht auswählen, blockiert Personal Firewall alle Pinganforderungen und zeichnet die Pingsignale im Protokoll für eingehende Ereignisse auf.

- **Änderung der Personal Firewall-Einstellungen für eine eingeschränkte Anzahl an Benutzern zulassen** – Wenn auf Ihrem Computer Windows XP oder Windows 2000 Professional mit mehreren Benutzern ausgeführt wird, wählen Sie diese Option aus, damit auch XP-Benutzer mit eingeschränkten Rechten die Einstellungen für Personal Firewall ändern können.

5 Klicken Sie auf **OK**, wenn Sie alle gewünschten Änderungen vorgenommen haben.

Testen von McAfee Personal Firewall Plus

Sie können Ihre Personal Firewall-Installation auf mögliche Sicherheitslücken bezüglich Eindringen und verdächtige Aktivitäten testen.

So testen Sie Ihre Personal Firewall-Installation mit dem McAfee-Symbol in der Taskleiste:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, und wählen Sie **Firewall testen** aus.

Personal Firewall öffnet Internet Explorer und ruft die Website http://www.hackerwatch.org/ auf, eine von McAfee gepflegte Website. Folgen Sie den Anweisungen auf der Testseite von HackerWatch.org, um Personal Firewall zu testen.

Verwenden von McAfee Personal Firewall Plus

So öffnen Sie Personal Firewall:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend einen Task aus.

Informationen zur Seite "Zusammenfassung"

Die Personal Firewall-Zusammenfassung enthält vier Zusammenfassungsseiten:

- Hauptübersicht
- Anwendungsübersicht
- Ereignisübersicht
- Zusammenfassung zu HackerWatch

Die Seiten **Zusammenfassung** enthalten unterschiedliche Berichte zu kürzlich eingegangenen Ereignissen, dem Anwendungsstatus sowie der von HackerWatch.org gemeldeten weltweiten Eindringaktivität. Außerdem finden Sie hier Links zu Tasks, die in Personal Firewall häufig ausgeführt werden.

So öffnen Sie die **Hauptübersicht** in Personal Firewall:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Zusammenfassung** (Abbildung 4-1) aus.

McAfee® Personal Firewall Plus
Datei Bearbeiten Anzeigen Ereignis Hilfe
personalfirewallplus
Schließen
Einstellungen
Hilfe
Hauptübersicht (Ansicht ändern)
Zusammenfassung
Internetanwendungen
Eingehende Ereignisse
Optionen
Für Ihre Firewall gelten derzeit folgende Einstellungen: Standardsicherheit.
3 neue Ereignisse wurden heute blockiert.
0 Anwendungsregeln wurden vor kurzem geändert.
Neues
Letzte Aktualisierung: 18.07.2005 11:05:22
Der Internetzugriff für das Programm Server wurde gesperrt. Diese Anwendung kann nicht mehr mit dem Internet kommunizieren.
Weitere Informationen anzeigen
Letztes Ereignis
Letzte Aktualisierung: 18.07.2005 11:06:32
Ein Computer, mit dem Sie unter der IP-Adresse 192.168.1.40 kommuniziert haben, hat versucht, auf einen anderen als den erwarteten Anschluss (UDP Anschluss 1483) zuzugreifen.
Dieses Ereignis verfolgen
Diese IP-Adresse als vertrauenswürdig einstufen
Täglicher Bericht
Täglicher Bericht über die Gesamtzahl der blockierten eingehenden Ereignisse.
Heute 3
Diese Woche 3
Diesen Monat 72
Aktive Anwendungen
Liste der derzeit in Ihrem System ausgeführten Anwendungen.
Windows Media Player
McAfee Personal Firewall...
Internet Explorer
Häufige Tasks
Aktuellen Internetverkehr anzeigen
Firewall-Einstellungen ändern
Online-Hilfe anzeigen
Standardsicherheit
IP-Adresse: 192.168.1.44 Netzwerkmaske: 255.255.255.0

Abbildung 4-1. Seite "Hauptübersicht"

Klicken Sie auf folgende Elemente, um zu den unterschiedlichen Zusammenfassungsseiten zu gelangen:

Element	Beschreibung
Ansicht ändern	Klicken Sie auf **Ansicht ändern**, um eine Liste von Zusammenfassungsseiten zu öffnen. Wählen Sie in der Liste eine Zusammenfassung aus, die angezeigt werden soll.
Pfeil nach rechts	Klicken Sie auf den Pfeil nach rechts, um die nächste Zusammenfassungsseite anzuzeigen.
Pfeil nach links	Klicken Sie auf den Pfeil nach links, um die vorherige Zusammenfassungsseite anzuzeigen.
Home	Klicken Sie auf das Symbol für die Startseite, um zur Seite **Hauptübersicht** zurückzukehren.

Auf der Seite **Hauptübersicht** stehen die folgenden Informationen:

Element	Beschreibung
Sicherheitseinstellung	Am Sicherheitseinstellungsstatus können Sie erkennen, welche Sicherheitsstufe für die Firewall festgelegt ist. Klicken Sie auf den Link, um die Sicherheitsstufe zu ändern.
Blockierte Ereignisse	Hier wird die Anzahl der Ereignisse angezeigt, die am aktuellen Tag blockiert wurden. Klicken Sie auf den Link, um Details zu dem Ereignis von der Seite **Eingehende Ereignisse** anzuzeigen.
Änderungen von Anwendungsregeln	Hier wird die Anzahl der Anwendungsregeln angezeigt, die kürzlich geändert wurden. Klicken Sie auf den Link, um die Liste zugelassener und blockierter Anwendungen anzuzeigen und Anwendungsberechtigungen zu ändern.
Neues	Unter **Neues** wird die Anwendung angezeigt, der zuletzt uneingeschränkter Zugriff auf das Internet gewährt wurde.
Letztes Ereignis	Unter **Letztes Ereignis** werden die letzten eingehenden Ereignisse angezeigt. Sie können auf einen Link klicken, um das Ereignis zu verfolgen oder um der IP-Adresse zu vertrauen. Wenn Sie einer IP-Adresse vertrauen, darf sämtlicher von dieser IP-Adresse stammender Datenverkehr an Ihrem Computer ankommen.
Täglicher Bericht	Unter **Täglicher Bericht** wird die Anzahl der eingehenden Ereignisse angezeigt, die von Personal Firewall am aktuellen Tag, in der aktuellen Woche oder im aktuellen Monat blockiert wurden. Klicken Sie auf den Link, um Details zu dem Ereignis von der Seite **Eingehende Ereignisse** anzuzeigen.
Aktive Anwendungen	Unter **Aktive Anwendungen** werden die Anwendungen angezeigt, die zurzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um die IP-Adressen anzuzeigen, zu denen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie auf einen Link unter **Häufige Tasks**, um auf Personal Firewall-Seiten die Aktivitäten der Firewall anzuzeigen bzw. Tasks durchzuführen.

So öffnen Sie die Seite **Anwendungsübersicht**:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Zusammenfassung** aus.
2. Klicken Sie auf **Ansicht ändern**, und wählen dann **Anwendungsübersicht** aus.

Auf der Seite **Anwendungsübersicht** stehen die folgenden Informationen:

Element	Beschreibung
Datenverkehrsmonitor	Der **Datenverkehrsmonitor** zeigt eingehende und ausgehende Internetverbindungen der vergangenen 15 Minuten an. Klicken Sie auf das Diagramm, um Details zur Datenverkehrsüberwachung anzuzeigen.
Aktive Anwendungen	Unter **Aktive Anwendungen** wird die Bandbreitennutzung der aktivsten Anwendungen des Computers in den letzten 24 Stunden angegeben. **Anwendung** – Die Anwendung, die auf das Internet zugreift. **%** – Der Prozentsatz an Bandbreite, der von der Anwendung genutzt wird. **Berechtigungen** – Der Typ von Internetzugriff, der für die Anwendung zulässig ist. **Regel erstellt am** – Der Zeitpunkt, zu dem die Anwendungsregel erstellt wurde.
Neues	Unter **Neues** wird die Anwendung angezeigt, der zuletzt uneingeschränkter Zugriff auf das Internet gewährt wurde.
Aktive Anwendungen	Unter **Aktive Anwendungen** werden die Anwendungen angezeigt, die zurzeit auf Ihrem Computer ausgeführt werden und auf das Internet zugreifen. Klicken Sie auf eine Anwendung, um die IP-Adressen anzuzeigen, zu denen die Anwendung eine Verbindung herstellt.
Häufige Tasks	Klicken Sie auf einen Link in **Häufige Tasks**, um auf Personal Firewall-Seiten den Anwendungsstatus anzuzeigen bzw. anwendungsbezogene Tasks durchzuführen.

So öffnen Sie die Seite **Ereignis-Zusammenfassung**:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Zusammenfassung** aus.

2 Klicken Sie auf **Ansicht ändern**, und wählen Sie dann **Ereignisübersicht** aus.

Auf der Seite **Ereignisübersicht** stehen die folgenden Informationen:

Element	Beschreibung
Anschlussvergleich	Unter **Anschlussvergleich** wird ein Kreisdiagramm der Anschlüsse in Ihrem Computer angezeigt, auf die in den letzten 30 Tagen am häufigsten versucht wurde zuzugreifen. Sie können auf einen Anschlussnamen klicken, um Details von der Seite **Eingehende Ereignisse** anzuzeigen. Sie können den Mauszeiger auch über die Anschlussnummer bewegen, um eine Beschreibung des Anschlusses einzublenden.
Hauptverursacher	**Hauptverursacher** zeigt die am häufigsten blockierten IP-Adressen und für jede Adresse den Zeitpunkt des letzten eingehenden Ereignisses sowie die Gesamtzahl der eingehenden Ereignisse pro Adresse in den letzten dreißig Tagen. Klicken Sie auf ein Ereignis, um Details zu diesem Ereignis von der Seite **Eingehende Ereignisse** anzuzeigen.
Täglicher Bericht	Unter **Täglicher Bericht** wird die Anzahl der eingehenden Ereignisse angezeigt, die von Personal Firewall am aktuellen Tag, in der aktuellen Woche oder im aktuellen Monat blockiert wurden. Klicken Sie auf eine Zahl, um Ereignisdetails aus dem Protokoll für eingehende Ereignisse anzuzeigen.
Letztes Ereignis	Unter **Letztes Ereignis** werden die letzten eingehenden Ereignisse angezeigt. Sie können auf einen Link klicken, um das Ereignis zu verfolgen oder um der IP-Adresse zu vertrauen. Wenn Sie einer IP-Adresse vertrauen, darf sämtlicher von dieser IP-Adresse stammender Datenverkehr an Ihrem Computer ankommen.
Häufige Tasks	Klicken Sie auf einen Link in **Häufige Tasks**, um auf den Personal Firewall-Seiten Ereignisdetails anzuzeigen bzw. ereignisbezogene Tasks durchzuführen.

So öffnen Sie die Seite **Zusammenfassung zu HackerWatch**:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie anschließend **Zusammenfassung** aus.
2. Klicken Sie auf **Ansicht ändern**, und wählen Sie dann **Zusammenfassung zu HackerWatch** aus.

Auf der Seite **Zusammenfassung zu HackerWatch** stehen die folgenden Informationen:

Element	Beschreibung
Weltweite Aktivität	Unter **Weltweite Aktivität** wird eine Weltkarte angezeigt, in der die von HackerWatch.org überwachten und in letzter Zeit blockierten Aktivitäten angezeigt werden. Klicken Sie auf die Karte, um eine Analyse globaler Bedrohungen in HackerWatch.org zu öffnen.
Ereignisverfolgung	Unter **Ereignisverfolgung** wird die Anzahl der eingehenden Ereignisse angegeben, die an HackerWatch.org übermittelt wurden.
Globale Anschlussaktivität	Unter **Globale Anschlussaktivität** werden die Anschlüsse angegeben, die innerhalb der letzten fünf Tage am häufigsten eine mögliche Bedrohung dargestellt haben. Klicken Sie auf einen Anschluss, um die Anschlussnummer und -beschreibung anzuzeigen.
Häufige Tasks	Klicken Sie auf einen Link in **Häufige Tasks**, um zu den HackerWatch.org-Seiten zu gelangen, auf denen Sie ausführlichere Informationen zur weltweiten Hackeraktivität erhalten.

Informationen zur Seite "Internetanwendungen"

Auf der Seite **Internetanwendungen** können Sie eine Liste der zugelassenen und blockierten Anwendungen anzeigen:

So starten Sie die Seite **Internetanwendungen**:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Anwendungen** (Abbildung 4-2) aus.

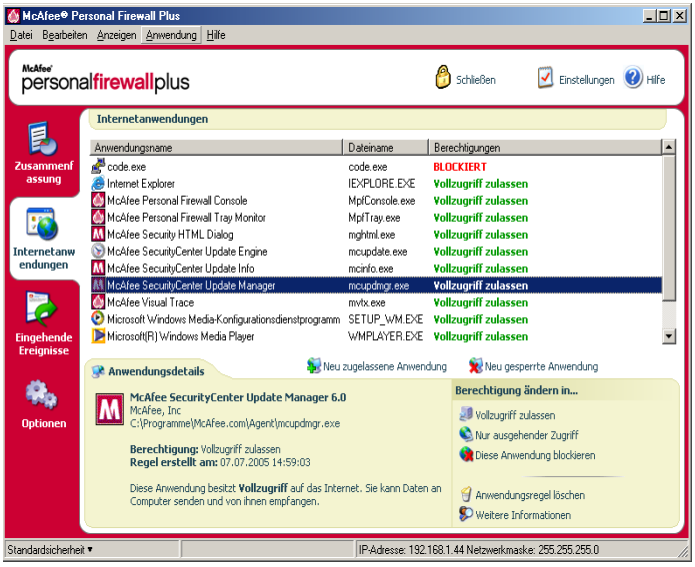


Abbildung 4-2. Seite "Internetanwendungen"

Auf der Seite **Internetanwendungen** stehen die folgenden Informationen:

- Anwendungsnamen
- Dateinamen
- Aktuelle Berechtigungsstufen
- Anwendungsdetails: Anwendungsname und -version, Firmenname, Pfadname, Berechtigung, Zeitstempel und Erläuterungen der Berechtigungstypen

Ändern von Anwendungsregeln

Mit Personal Firewall können Sie die Zugriffsregeln für Anwendungen ändern.

So ändern Sie eine Anwendungsregel:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Internetanwendungen** aus.
2. Klicken Sie in der Liste **Internetanwendungen** mit der rechten Maustaste auf die Anwendungsregel einer Anwendung, und wählen Sie eine andere Zugriffsstufe aus:
   - **Vollzugriff zulassen** – Die Anwendung darf sowohl eingehende als auch ausgehende Internetverbindungen aufbauen.
   - **Nur ausgehender Zugriff** – Die Anwendung darf nur ausgehende Internetverbindungen aufbauen.
   - **Diese Anwendung blockieren** – Die Anwendung darf keinerlei Internetzugriffe durchführen.

     HINWEIS
     Zuvor blockierte Anwendungen werden auch weiterhin blockiert, wenn die Sicherheitseinstellung der Firewall auf **Offen (Kein Filter)** oder **Verbindung schließen** gesetzt ist. Wenn Sie dies nicht möchten, können Sie entweder die Zugriffsregel der Anwendung in **Vollzugriff zulassen** ändern oder die Berechtigungsregel **Diese Anwendung blockieren** aus der Liste **Internetanwendungen** löschen.

So löschen Sie eine Anwendungsregel:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Internetanwendungen** aus.
2. Klicken Sie in der Liste **Internetanwendungen** mit der rechten Maustaste auf die Anwendungsregel, und wählen Sie dann **Anwendungsregel löschen** aus.

Wenn die Anwendung das nächste Mal Internetzugriff anfordert, können Sie ihre Berechtigungsstufe so festlegen, dass sie der Liste erneut hinzugefügt wird.

Zulassen und Blockieren von Internetanwendungen

So ändern Sie die Liste der zugelassenen und blockierten Internetanwendungen:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Internetanwendungen** aus.

2 Klicken Sie auf der Seite **Internetanwendungen** auf eine der folgenden Optionen:

- **Neu zugelassene Anwendung** – Hiermit gewähren Sie einer Anwendung vollständigen Internetzugriff.
- **Neu gesperrte Anwendung** – Hiermit unterbinden Sie den Internetzugriff einer Anwendung.
- **Anwendungsregel löschen** – Hiermit entfernen Sie eine Anwendungsregel.

Informationen zur Seite "Eingehende Ereignisse"

Auf der Seite **Eingehende Ereignisse** können Sie das Protokoll eingehender Ereignisse anzeigen, das erstellt wird, wenn Personal Firewall unangeforderte Internetverbindungen blockiert.

So starten Sie die Seite **Eingehende Ereignisse**:

- Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** (Abbildung 4-3) aus.

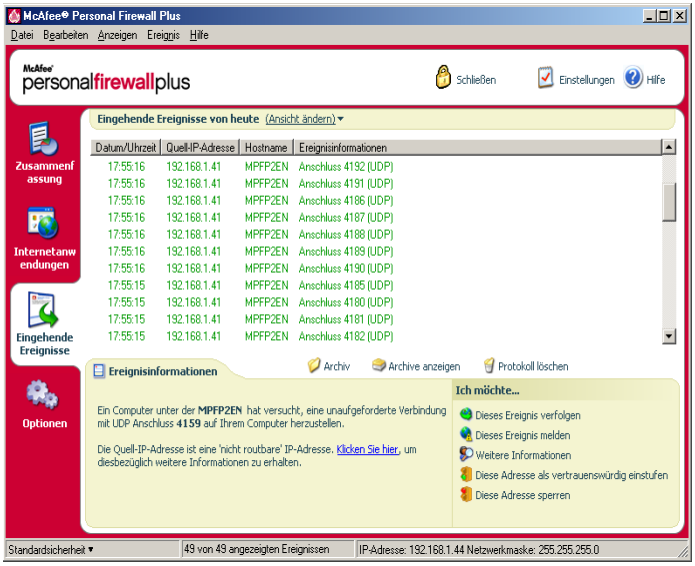

McAfee® Personal Firewall Plus
Datei Bearbeiten Anzeigen Ereignis Hilfe
personalfirewallplus
Schließen
Einstellungen
Hilfe
Zusammenfassung
Internetanwendungen
Eingehende Ereignisse
Optionen
Eingehende Ereignisse von heute (Ansicht ändern)
Datum/Uhrzeit | Quell-IP-Adresse | Hostname | Ereignisinformationen
17:55:16 192.168.1.41 MPFP2EN Anschluss 4192 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4191 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4186 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4187 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4188 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4189 (UDP)
17:55:16 192.168.1.41 MPFP2EN Anschluss 4190 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4185 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4180 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4181 (UDP)
17:55:15 192.168.1.41 MPFP2EN Anschluss 4182 (UDP)
Ereignisinformationen
Archiv
Archive anzeigen
Protokoll löschen
Ein Computer unter der MPFP2EN hat versucht, eine unaufgeforderte Verbindung mit UDP Anschluss 4159 auf Ihrem Computer herzustellen.
Die Quell-IP-Adresse ist eine 'nicht routbare' IP-Adresse. Klicken Sie hier, um diesbezüglich weitere Informationen zu erhalten.
Ich möchte...
Dieses Ereignis verfolgen
Dieses Ereignis melden
Weitere Informationen
Diese Adresse als vertrauenswürdig einstufen
Diese Adresse sperren
Standardsicherheit
49 von 49 angezeigten Ereignissen
IP-Adresse: 192.168.1.44 Netzwerkmaske: 255.255.255.0

Abbildung 4-3. Seite "Eingehende Ereignisse"

Auf der Seite **Eingehende Ereignisse** finden die folgenden Informationen:

- Zeitstempel
- IP-Quelladressen
- Hostnamen
- Dienst- oder Anwendungsnamen
- Details zum Ereignis: Verbindungstypen, Verbindungsanschlüsse, Hostnamen oder IP-Adresse und Erläuterungen zu Anschlussereignissen

Grundlegendes zu Ereignissen

Informationen zu IP-Adressen

IP-Adressen bestehen aus Zahlen, genauer gesagt aus vier verschiedenen Zahlenblöcken zwischen 0 und 255. Diese Zahlen identifizieren eine bestimmte Stelle, an die der Datenverkehr im Internet weitergeleitet werden kann.

IP-Adresstypen

Einige IP-Adressen werden aus verschiedenen Gründen nicht verwendet:

Nicht routbare IP-Adressen – Diese werden auch als "Privater IP-Adressraum" bezeichnet. Diese IP-Adressen können im Internet nicht verwendet werden. Private IP-Blöcke sind 10.x.x.x, 172.16.x.x bis 172.31.x.x und 192.168.x.x.

Loopback-IP-Adressen – Loopback-Adressen werden zu Testzwecken verwendet. Datenpakete, die an diesen IP-Adressblock gesendet werden, kehren sofort wieder zu dem Gerät zurück, von dem das Paket generiert wurde. Da an diese IP-Adressen gerichtete Datenpakete das Gerät überhaupt nicht verlassen, werden diese Adressen hauptsächlich für Hardware- und Softwaretests verwendet. Der Loopback-IP-Block beginnt mit 127.x.x.x.

Null-IP-Adresse – Dies ist eine ungültige Adresse. Wird dieser Adresstyp erkannt, weist Personal Firewall darauf hin, dass der Datenverkehr eine leere IP-Adresse verwendet hat. Häufig ist dies ein Hinweis darauf, dass der Absender absichtlich die Quelle des Datenverkehrs verschleiert. Der Absender kann keine Antwort auf den Datenverkehr erhalten, es sei denn, das Paket wird von einer Anwendung empfangen, die den Paketinhalt (d. h. die anwendungsspezifischen Anweisungen) versteht und damit entsprechend umgehen kann. Jede Adresse, die mit 0 beginnt (0.x.x.x), ist eine Null-Adresse. Beispiel: 0.0.0.0 ist eine Null-IP-Adresse.

Ereignisse von 0.0.0.0

Für Ereignisse, die von der IP-Adresse 0.0.0.0 stammen, gibt es zwei mögliche Ursachen. Die erste und häufigste Ursache besteht darin, dass Ihr Computer ein fehlerhaftes Paket erhalten hat. Das Internet ist nicht immer hundertprozentig zuverlässig, und fehlerhafte Pakete sind durchaus möglich. Da Personal Firewall die Pakete vor der TCP/IP-Validierung erhält, kann es solche Pakete möglicherweise als Ereignis melden.

Die zweite Ursache besteht darin, dass die IP-Quelladresse gefälscht oder "gespooft" wurde. Gefälschte Pakete können ein Anzeichen dafür sein, dass jemand Ihren Computer auf Trojaner überprüft. Personal Firewall blockiert solche Aktivitäten, so dass Ihr Computer sicher ist.

Ereignisse von 127.0.0.1

Manchmal wird von Ereignissen als IP-Quelladresse 127.0.0.1 angegeben. Diese Adresse wird auch Loopbackadresse oder "localhost" genannt.

Viele seriöse Programme verwenden die Loopbackadresse zur Kommunikation zwischen den Komponenten. Beispielsweise können viele private E-Mail- oder Webserver über eine Weboberfläche konfiguriert werden. Wenn Sie auf die Weboberfläche zugreifen möchten, geben Sie in Ihrem Webbrowser “http://localhost/” ein.

Personal Firewall lässt Datenverkehr von diesen Programmen zu. Wenn also Ereignisse mit der IP-Adresse 127.0.0.1 angezeigt werden, bedeutet dies in der Regel, dass die IP-Quelladresse gefälscht ist. Gefälschte Pakete weisen meist darauf hin, dass Ihr Computer von einem anderen auf Trojaner überprüft wird. Personal Firewall blockiert solche Eindringversuche, so dass Ihr Computer sicher ist.

Bei einigen Programmen (insbesondere Netscape ab Version 6.2) ist es jedoch erforderlich, dass Sie die Adresse 127.0.0.1 zur Liste **Vertrauenswürdige IP-Adressen** hinzufügen. Die Komponenten dieser Programme kommunizieren so miteinander, dass Personal Firewall nicht bestimmen kann, ob es sich um einen lokalen Datenverkehr handelt oder nicht.

Bei Netscape 6.2 können Sie zum Beispiel Ihre Buddyliste nicht verwenden, wenn Sie die Adresse 127.0.0.1 nicht als vertrauenswürdig einstufen. Wenn Sie also Datenverkehr von 127.0.0.1 bemerken und alle Anwendungen auf Ihrem Computer normal funktionieren, können Sie diesen Datenverkehr sicherheitshalber blockieren. Wenn jedoch bei einem Programm (wie Netscape) Probleme auftreten, fügen Sie 127.0.0.1 zur Liste **Vertrauenswürdige IP-Adressen** in Personal Firewall hinzu.

Wird das Problem durch die Aufnahme von 127.0.0.1 in die Liste der vertrauenswürdigen IP-Adressen behoben, müssen Sie die Vor- und Nachteile abwägen: Wenn Sie die Adresse 127.0.0.1 als vertrauenswürdig einstufen, funktioniert zwar das Programm, allerdings erhöht sich die Gefahr, dass Angriffe mit gefälschten Adressen ausgeführt werden. Wenn Sie diese Adresse nicht als vertrauenswürdig einstufen, funktioniert das Programm nicht, dafür bleiben Sie vor bestimmtem feindlichen Datenverkehr geschützt.

Ereignisse von Computern in Ihrem lokalen Netzwerk (LAN)

Ereignisse können auch von Computern in Ihrem LAN (Local Area Network) generiert werden. Um anzuzeigen, dass diese Ereignisse von Ihrem Netzwerk erzeugt werden, stellt sie Personal Firewall grün dar.

Für die meisten Unternehmens-LANs sollten Sie im Dialogfeld **Vertrauenswürdige IP-Adressen** das Kontrollkästchen **Alle Computer in meinem LAN als vertrauenswürdig einstufen** aktivieren.

In einigen Situationen kann Ihr "lokales" Netzwerk genauso gefährlich sein wie das Internet – insbesondere dann, wenn Ihr Computer an ein Netzwerk mit einer hohen Bandbreite (z. B. DSL oder Kabelmodem) angeschlossen ist. Aktivieren Sie das Kontrollkästchen **Alle Computer in meinem LAN als vertrauenswürdig einstufen** in diesem Fall nicht. Fügen Sie stattdessen die IP-Adressen Ihrer lokalen Computer zur Liste **Vertrauenswürdige IP-Adressen** hinzu.

Ereignisse von privaten IP-Adressen

IP-Adressen im Format 192.168.xxx.xxx, 10.xxx.xxx.xxx und 172.16.0.0 bis 172.31.255.255 werden als nicht routbare oder private IP-Adressen bezeichnet. Diese IP-Adressen sollten Ihr Netzwerk nie verlassen und können in der Regel als vertrauenswürdig angesehen werden.

Der Block 192.168.xxx.xxx wird im Zusammenhang mit Microsoft Internet Connection Sharing (ICS) verwendet. Wenn Sie ICS verwenden und Ereignisse von diesem IP-Block angezeigt werden, können Sie die IP-Adresse 192.168.255.255 in die Liste **Vertrauenswürdige IP-Adressen** aufnehmen. Dadurch wird der gesamte Block 192.168.xxx.xxx als vertrauenswürdig eingestuft.

Wenn Sie sich nicht in einem privaten Netzwerk befinden und Ereignisse von diesen IP-Bereichen angezeigt werden, bedeutet dies, dass die IP-Quelladresse möglicherweise gefälscht ist. Gefälschte Pakete sind oft ein Zeichen dafür, dass jemand nach Trojanern sucht. Denken Sie immer daran, dass Personal Firewall diesen Versuch blockiert hat und Ihr Computer somit sicher ist.

Da private IP-Adressen in jedem Netzwerk auf andere Computer verweisen, würde es wenig Sinn machen, derartige Ereignisse zu melden.

Anzeigen von Ereignissen im Protokoll für eingehende Ereignisse

Das Protokoll für eingehende Ereignisse zeigt Ereignisse auf verschiedene Weise an. In der Standardansicht werden nur Ereignisse des aktuellen Tags angezeigt. Sie können auch die in der vergangenen Woche aufgetretenen Ereignisse oder das gesamte Protokoll anzeigen.

Außerdem können Sie mit Personal Firewall eingehende Ereignisse von bestimmten Tagen, bestimmten Internetadressen (IP-Adressen) oder Ereignisse mit identischen Ereignisinformationen anzeigen.

Wenn Sie Informationen über ein bestimmtes Ereignis anzeigen möchten, klicken Sie auf das Ereignis, und zeigen Sie die Informationen im Bereich **Ereignisinformationen** an.

Anzeigen der Ereignisse des heutigen Tages

Verwenden Sie diese Option, um die Ereignisse des heutigen Tages zu überprüfen.

So zeigen Sie die Ereignisse des heutigen Tages an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf einen Eintrag, und klicken Sie dann auf **Ereignisse von heute anzeigen**.

Anzeigen der Ereignisse aus dieser Woche

Verwenden Sie diese Option, um die Ereignisse aus dieser Woche anzuzeigen.

So zeigen Sie die Ereignisse aus dieser Woche an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf einen Eintrag, und klicken Sie dann auf **Ereignisse aus dieser Woche anzeigen**.

Anzeigen des gesamten Protokolls eingehender Ereignisse

Verwenden Sie diese Option, um sämtliche Ereignisse anzuzeigen.

So zeigen Sie alle Ereignisse im Protokoll eingehender Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und klicken Sie dann auf **Eingehende Ereignisse**.

2 Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf einen Eintrag, und klicken Sie dann auf **Vollständiges Protokoll anzeigen**.

Es werden alle Ereignisse aus dem Protokoll für eingehende Ereignisse angezeigt.

Anzeigen der Ereignisse eines bestimmten Tages

Verwenden Sie diese Option, um die Ereignisse eines bestimmten Tages anzuzeigen.

So zeigen Sie die Ereignisse eines bestimmten Tages an:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.

2 Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf einen Eintrag, und klicken Sie dann auf **Nur Ereignisse des ausgewählten Tages anzeigen**.

Anzeigen der Ereignisse von einer bestimmten Internetadresse

Verwenden Sie diese Option, um andere Ereignisse anzuzeigen, die von einer bestimmten Internetadresse stammen.

So zeigen Sie Ereignisse von einer bestimmten Internetadresse an:

1 Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.

2 Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf einen Eintrag, und klicken Sie dann auf **Nur Ereignisse von einer bestimmten Internetadresse anzeigen**.

Anzeigen von Ereignissen, die über identische Ereignisinformationen verfügen

Verwenden Sie diese Option, wenn Sie andere Ereignisse aus dem Protokoll der eingehenden Ereignisse anzeigen möchten, bei denen in der Spalte **Ereignisinformationen** dieselben Informationen wie bei dem von Ihnen ausgewählten Ereignis stehen. Sie können auf diese Weise feststellen, wie oft dieses Ereignis stattgefunden hat, und überprüfen, ob es von derselben Quelle stammt. Die Spalte **Ereignisinformationen** enthält eine Beschreibung des Ereignisses und, falls bekannt, das Programme bzw. den Dienst, von dem dieser Anschluss üblicherweise verwendet wird.

So zeigen Sie Ereignisse mit identischen Ereignisinformationen an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und klicken Sie auf **Eingehende Ereignisse**.
2. Klicken Sie im Protokoll der eingehenden Ereignisse mit der rechten Maustaste auf einen Eintrag, und klicken Sie dann auf **Nur Ereignisse mit identischen Ereignisinformationen anzeigen**.

Reagieren auf eingehende Ereignisse

Zusätzlich zur Überprüfung von Details zu Ereignissen im Protokoll eingehender Ereignisse können Sie eine visuelle Verfolgung der IP-Adressen zu Ereignissen im Protokoll eingehender Ereignisse durchführen oder Ereignisdetails auf der Website der Anti-Hacker-Online-Community HackerWatch.org anzeigen.

Verfolgen eines ausgewählten Ereignisses

Sie können versuchen, eine visuelle Verfolgung der IP-Adressen für ein Ereignis im Protokoll eingehender Ereignisse durchzuführen.

So verfolgen Sie ein ausgewähltes Ereignis:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie im Protokoll für eingehende Ereignisse auf das zu verfolgende Ereignis und anschließend auf **Dieses Ereignis verfolgen**. Sie können auch auf ein Ereignis doppelklicken, um es zu verfolgen.

Standardmäßig beginnt Personal Firewall eine visuelle Verfolgung mit dem integrierten Programm Personal Firewall Visual Trace.

Abrufen von Empfehlungen von HackerWatch.org

So rufen Sie Empfehlungen von HackerWatch.org ab:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie **Eingehende Ereignisse** aus.
2. Wählen Sie den Eintrag des Ereignisses auf der Seite **Eingehende Ereignisse** aus, und klicken Sie dann im Bereich **Ich möchte** auf **Weitere Informationen**.

Ihr Standardwebbrowser wird gestartet und die Website HackerWatch.org geöffnet, von der Sie Informationen zum Ereignistyp abrufen können und eine Empfehlung erhalten, ob Sie das Ereignis melden sollen.

Melden eines Ereignisses

Wenn Sie ein Ereignis melden möchten, das Ihrer Meinung nach ein Angriff auf Ihren Computer war, gehen Sie folgendermaßen vor:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie auf das Ereignis, das Sie melden möchten, und klicken Sie dann im Bereich **Ich möchte** auf **Dieses Ereignis melden**.

Personal Firewall meldet das Ereignis unter Ihrer eindeutigen ID an HackerWatch.org.

Anmelden bei HackerWatch.org

Wenn Sie die Seite **Zusammenfassung** zum ersten Mal öffnen, fordert Personal Firewall bei HackerWatch.org eine eindeutige ID für Sie an. Sind Sie bereits ein eingetragener Benutzer, wird Ihre Anmeldung automatisch überprüft. Sind Sie ein neuer Benutzer, müssen Sie einen Benutzernamen sowie eine E-Mail-Adresse angeben und in der Bestätigungs-E-Mail von HackerWatch.org auf den Link zur Bestätigung klicken, damit Sie auf der Website die Funktionen zum Filtern und Senden von Ereignissen verwenden können.

Sie können Ereignisse auch ohne Überprüfung Ihrer Benutzer-ID an HackerWatch.org melden. Um Ereignisse zu filtern und als E-Mail an einen Freund zu senden, müssen Sie sich jedoch für den Dienst anmelden.

Wenn Sie sich angemeldet haben, können wir die von Ihnen übermittelten Hinweise Ihnen zuordnen und Sie benachrichtigen, wenn HackerWatch.org weitere Informationen von Ihnen benötigt oder Sie bestimmte Aktionen durchführen müssen. Eine Anmeldung ist außerdem erforderlich, da wir alle eingegangenen Informationen bezüglich ihrer Nützlichkeit bestätigen müssen.

Alle E-Mail-Adressen werden von HackerWatch.org als vertraulich behandelt. Wenn ein ISP weitere Informationen anfordert, wird diese Anfrage über HackerWatch.org geleitet; Ihre E-Mail-Adresse wird niemals bekannt gegeben.

Einstufen einer Adresse als vertrauenswürdig

Sie können die Seite **Eingehende Ereignisse** verwenden, um eine IP-Adresse zur Liste **Vertrauenswürdige IP-Adressen** hinzuzufügen, um eine ständige Verbindung zu erlauben.

Wenn auf der Seite **Eingehende Ereignisse** ein Ereignis angezeigt wird, das eine IP-Adresse enthält, die von Ihnen zugelassen werden muss, können Sie festlegen, dass Personal Firewall Verbindungen von dieser Adresse jederzeit zulassen soll.

So fügen Sie eine IP-Adresse zur Liste **Vertrauenswürdige IP-Adressen** hinzu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie mit der rechten Maustaste auf das Ereignis, dessen IP-Adresse als vertrauenswürdig eingestuft werden soll, und klicken Sie dann auf **Der Quell-IP-Adresse vertrauen**.

Überprüfen Sie, ob die im Dialogfeld **Diese Adresse als vertrauenswürdig einstufen** angezeigte IP-Adresse korrekt ist, und klicken Sie dann auf **OK**. Die IP-Adresse wird der Liste **Vertrauenswürdige IP-Adressen** hinzugefügt.

So überprüfen Sie, ob die IP-Adresse hinzugefügt wurde:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie **Optionen** aus.
2. Klicken Sie auf das Symbol für vertrauenswürdige und gesperrte IP-Adressen, und klicken Sie dann auf die Registerkarte **Vertrauenswürdige IP-Adressen**.

Die IP-Adresse wird in der Liste **Vertrauenswürdige IP-Adressen** markiert angezeigt.

Sperren einer Adresse

Wenn eine IP-Adresse in Ihrem Protokoll eingehender Ereignisse angezeigt wird, bedeutet dies, dass Datenverkehr von dieser Adresse blockiert wurde. Folglich stellt das Sperren einer Adresse keinen zusätzlichen Schutz dar, es sei denn, der Computer verfügt über Anschlüsse, die über die Funktion "Systemdienste" absichtlich geöffnet werden, bzw. auf dem Computer befindet sich eine Anwendung, die für den Empfang von Datenverkehr berechtigt ist.

Fügen Sie der Liste gesperrter IP-Adressen nur dann eine IP-Adresse hinzu, wenn Sie über mindestens einen Anschluss verfügen, der absichtlich geöffnet ist, und Sie Grund zur Annahme haben, dass der Zugriff unterbunden werden muss.

Wenn auf der Seite **Eingehende Ereignisse** ein Ereignis angezeigt wird, das eine IP-Adresse enthält, die Sie sperren möchten, können Sie Personal Firewall so konfigurieren, dass Verbindungen von dieser Adresse in jedem Fall unterbunden werden.

Auf der Seite **Eingehende Ereignisse**, auf der alle IP-Adressen mit eingehendem Internetverkehr aufgeführt sind, können Sie eine IP-Adresse sperren, von der Sie vermuten, dass sie Ausgangspunkt von verdächtigen oder unerwünschten Internet-Aktivitäten ist.

So fügen Sie eine IP-Adresse zur Liste **Gesperrte IP-Adressen** hinzu:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Auf der Seite **Eingehende Ereignisse** sind alle IP-Adressen mit eingehendem Internetverkehr aufgeführt. Wählen Sie eine IP-Adresse aus, und gehen Sie dann auf eine der folgenden Weisen vor:
   - Klicken Sie mit der rechten Maustaste auf die IP-Adresse, und wählen Sie dann **Quell-IP-Adresse sperren** aus.
   - Klicken Sie im Menü **Ich möchte** auf **Diese Adresse sperren**.
3. Verwenden Sie eine oder mehrere der folgenden Einstellungen im Dialogfeld **Regel für gesperrte IP-Adresse hinzufügen**, um die Regel für gesperrte IP-Adressen zu konfigurieren:
   - **Eine einzelne IP-Adresse** – Die IP-Adresse, die gesperrt werden soll. Standardmäßig ist hier die IP-Adresse eingetragen, die Sie auf der Seite **Eingehende Ereignisse** ausgewählt haben.
   - **Ein IP-Adressbereich** – Alle IP-Adressen zwischen den beiden Adressen, die Sie in den Feldern **Von IP-Adresse** und **An IP-Adresse** angeben.
   - **Ablaufdatum für diese Regel festlegen auf** – Datum und Uhrzeit, wann die Regel zum Sperren der IP-Adresse abläuft. Wählen Sie das Datum und die Uhrzeit aus den entsprechenden Dropdown-Menüs aus.
   - **Beschreibung** – Hier können Sie optional eine Beschreibung der neuen Regel eingeben.
   - Klicken Sie auf **OK**.
4. Klicken Sie im Dialogfeld auf **Ja**, um Ihre Einstellung zu bestätigen. Klicken Sie auf **Nein**, um zum Dialogfeld **Regel für gesperrte IP-Adresse hinzufügen** zurückzukehren.

Wenn Personal Firewall ein Ereignis von einer gesperrten Internetverbindung erkennt, erhalten Sie eine Warnung gemäß der Vorgehensweise, die Sie auf der Seite **Warneinstellungen** festgelegt haben.

So überprüfen Sie, ob die IP-Adresse hinzugefügt wurde:

1. Klicken Sie auf die Registerkarte **Optionen**.
2. Klicken Sie auf das Symbol für vertrauenswürdige und gesperrte IP-Adressen, und klicken Sie dann auf die Registerkarte **Gesperrte IP-Adressen**.

Die IP-Adresse wird in der Liste **Gesperrte IP-Adressen** markiert angezeigt.

Verwalten des Protokolls eingehender Ereignisse

Auf der Seite **Eingehende Ereignisse** können Sie die Ereignisse im Protokoll eingehender Ereignisse verwalten, das erzeugt wird, wenn Personal Firewall unangeforderten Internetverkehr blockiert.

Archivieren des Protokolls eingehender Ereignisse

Sie können das aktuelle Protokoll für eingehende Ereignisse archivieren, um alle protokollierten eingehenden Ereignisse inklusive Datum und Uhrzeit, Quell-IPs, Hostnamen, Anschlüsse und Ereignisinformationen zu speichern. Sie sollten das Protokoll eingehender Ereignisse in regelmäßigen Abständen archivieren, um zu vermeiden, dass es zu umfangreich wird.

So archivieren Sie das Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie auf der Seite **Eingehende Ereignisse** auf **Archiv**.
3. Klicken Sie im Dialogfeld **Protokoll archivieren** auf **Ja**, um den Vorgang fortzusetzen.
4. Klicken Sie auf **Speichern**, um das Archiv im Standardverzeichnis zu speichern, oder wechseln Sie zu einem Speicherort, in dem Sie das Archiv speichern möchten.

HINWEIS
Standardmäßig archiviert Personal Firewall das Protokoll für eingehende Ereignisse automatisch. Verwenden Sie **Protokollierte Ereignisse automatisch archivieren** auf der Seite **Ereignisprotokolleinstellungen**, um diese Option zu aktivieren bzw. zu deaktivieren.

Anzeigen eines archivierten Protokolls eingehender Ereignisse

Sie können jedes Protokoll eingehender Ereignisse anzeigen, das Sie zu einem früheren Zeitpunkt archiviert haben. Das gespeicherte Archiv enthält Angaben wie Datum und Uhrzeit, Quell-IPs, Hostnamen, Anschlüsse und Ereignisinformationen zu den Ereignissen.

So zeigen Sie ein archiviertes Protokoll eingehender Ereignisse an:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie auf der Seite **Eingehende Ereignisse** auf **Archive anzeigen**.
3. Wählen Sie den Namen der Archivdatei aus, oder wechseln Sie zur gewünschten Archivdatei, und klicken Sie dann auf **Öffnen**.

Löschen des Inhalts des Protokolls eingehender Ereignisse

Sie können alle Informationen aus dem Protokoll eingehender Ereignisse löschen.

> **ACHTUNG**
> Gelöschte Inhalte können nicht wiederhergestellt werden. Wenn Sie glauben, das Ereignisprotokoll zukünftig noch zu benötigen, sollten Sie es stattdessen archivieren.

So löschen Sie den Inhalt des Protokolls eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie auf der Seite **Eingehende Ereignisse** auf **Protokoll löschen**.
3. Klicken Sie im Dialogfeld auf **Ja**, um den Inhalt des Protokolls zu löschen.

Kopieren eines Ereignisses in die Zwischenablage

Sie können ein Ereignis in die Zwischenablage kopieren, um es von dort aus in eine Textdatei im Windows-Editor einzufügen.

So kopieren Sie Ereignisse in die Zwischenablage:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.
2. Klicken Sie mit der rechten Maustaste auf das Ereignis im Protokoll eingehender Ereignisse.
3. Klicken Sie auf **Ausgewähltes Ereignis in Zwischenablage kopieren**.
4. Starten Sie den Editor.
   - Geben Sie in der Befehlszeile `notepad` (Editor) ein, oder klicken Sie auf die Schaltfläche **Start** in der Windows-Taskleiste, zeigen Sie auf **Programme**, dann auf **Zubehör**, und wählen Sie **Editor** aus.
5. Klicken Sie auf **Bearbeiten** und dann auf **Einfügen**. Der Ereignistext wird im Editor angezeigt. Wiederholen Sie diesen Schritt so oft, bis alle gewünschten Ereignisse kopiert wurden.
6. Speichern Sie die Datei an einem sicheren Ort.

Löschen eines ausgewähltes Ereignisses

Sie können Ereignisse aus dem Protokoll eingehender Ereignisse löschen.

So löschen Sie Ereignisse aus dem Protokoll eingehender Ereignisse:

1. Klicken Sie mit der rechten Maustaste auf das McAfee-Symbol in der Windows-Taskleiste, zeigen Sie auf **Personal Firewall**, und wählen Sie dann **Eingehende Ereignisse** aus.

2 Klicken Sie auf der Seite **Eingehende Ereignisse** auf den Eintrag des Ereignisses, das Sie löschen möchten.

3 Klicken Sie im Menü **Bearbeiten** auf **Ausgewähltes Ereignis löschen**. Das Ereignis wird aus dem Protokoll eingehender Ereignisse gelöscht.

Informationen zu Warnungen

Es wird dringend empfohlen, sich mit den Warntypen vertraut zu machen, mit denen Sie beim Arbeiten mit Personal Firewall in Berührung kommen werden. Lesen Sie die folgenden Informationen zu den vorhandenen Warntypen und den möglichen Reaktionen, damit Sie mit Warnungen sicher umgehen können.

HINWEIS
Empfehlungen zu Warnungen unterstützen Sie bei der richtigen Handhabung einer Warnung. Wenn Sie möchten, dass Warnungen auch Empfehlungen enthalten sollen, klicken Sie auf die Registerkarte **Optionen**, klicken Sie dann auf das Symbol **Warneinstellungen**, und wählen Sie dann in der Liste **Empfehlungen** entweder **Empfehlungen verwenden** (die Standardeinstellung) oder **Nur Empfehlungen anzeigen** aus.

Rote Warnmeldungen

Rote Warnmeldungen enthalten wichtige Informationen, die Ihre sofortige Aufmerksamkeit erfordern:

- **Internetanwendung blockiert** – Diese Warnung wird angezeigt, wenn Personal Firewall eine Anwendung daran hindert, auf das Internet zuzugreifen. Wenn beispielsweise eine Trojaner-Warnung angezeigt wird, verweigert McAfee dem entsprechenden Programm automatisch den Internetzugriff und empfiehlt Ihnen, den Computer auf Viren zu überprüfen.
- **Die Anwendung möchte auf das Internet zugreifen** – Diese Warnung wird angezeigt, wenn Personal Firewall Internet- oder Netzwerkverkehr bei neuen Anwendungen erkennt.
- **Die Anwendung wurde geändert** – Diese Warnung wird angezeigt, wenn Personal Firewall erkennt, dass eine Anwendung geändert wurde, der Sie zuvor Zugriff auf das Internet gewährt haben. Wenn Sie die entsprechende Anwendung in letzter Zeit nicht aktualisiert haben, sollten Sie vorsichtig sein, wenn Sie ihr Zugriff auf das Internet gewähren.

- **Die Anwendung fordert Serverzugriff an** – Diese Warnung wird angezeigt, wenn Personal Firewall erkennt, dass eine Anwendung, der Sie zuvor Zugriff auf das Internet gewährt haben, Internetzugriff als Server anfordert.

HINWEIS

Die Standardeinstellung von Windows XP SP2 für automatische Updates lädt Updates für das Windows-Betriebssystem und andere auf Ihrem Rechner ausgeführte Microsoft-Programme herunter und installiert diese, ohne dass Sie davon benachrichtigt werden. Wenn eine Anwendung durch ein solches automatisches Windows-Update geändert wurde, zeigt McAfee Personal Firewall beim nächsten Ausführen der betreffenden Microsoft-Anwendung eine Meldung an.

WICHTIG

Anwendungen, die Internetzugriff für Online-Produktupdates benötigen (z. B. McAfee-Dienste), müssen Sie diesen Zugriff gewähren, um sie auf dem neuesten Stand zu halten.

Warnung "Internetanwendung blockiert"

Wenn eine Trojaner-Warnung angezeigt wird (Abbildung 4-4), verweigert Personal Firewall dem entsprechenden Programm automatisch den Internetzugriff und empfiehlt Ihnen, den Computer auf Viren zu überprüfen. Ist McAfee VirusScan nicht installiert, können Sie McAfee SecurityCenter starten.

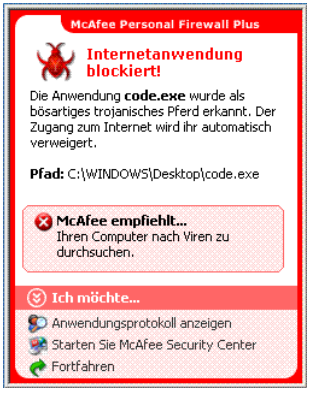

McAfee Personal Firewall Plus
Internetanwendung blockiert!
Die Anwendung code.exe wurde als bösartiges trojanisches Pferd erkannt. Der Zugang zum Internet wird ihr automatisch verweigert.
Pfad: C:\WINDOWS\Desktop\code.exe
McAfee empfiehlt...
Ihren Computer nach Viren zu durchsuchen.
Ich möchte...
Anwendungsprotokoll anzeigen
Starten Sie McAfee Security Center
Fortfahren

Abbildung 4-4. Warnung "Internetanwendung blockiert"

Zeigen Sie eine kurze Beschreibung des Ereignisses an, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten:

- Klicken Sie auf **Weitere Informationen**, um detaillierte Informationen zu dem Ereignis aus dem Protokoll eingehender Ereignisse anzuzeigen (weitere Informationen finden Sie unter *Informationen zur Seite "Eingehende Ereignisse"* auf Seite 103).
- Klicken Sie auf **Starten Sie McAfee Security Center**, um den Computer auf Viren zu überprüfen.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Auf abgehenden Zugriff beschränken,** um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).

Warnung "Die Anwendung möchte auf das Internet zugreifen"

Wenn Sie in den **Sicherheitseinstellungen** die Option **Standard** oder **Eingeschränkte** Sicherheit ausgewählt haben, zeigt Personal Firewall eine Warnung an (Abbildung 4-5), wenn Internet- oder Netzwerkverbindungen von neuen oder geänderten Anwendungen erkannt werden.

McAfee Personal Firewall Plus
Die Anwendung möchte auf das Internet zugreifen.
Das Programm Server fordert Zugriff auf das Internet an. Möchten Sie ihn gewähren?
Pfad: C:\WINDOWS\Desktop\server.exe \Server.exe
Ich möchte...
Zugriff gewähren
Zugriff einmal gewähren
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 4-5. Warnung "Die Anwendung möchte auf das Internet zugreifen"

Wenn eine Warnung eingeblendet wird, die zur Vorsicht beim Gewähren von Internetzugriff für die Anwendung rät, können Sie auf **Klicken Sie hier, um weitere Informationen anzuzeigen** klicken, um weitere Informationen zur Anwendung zu erhalten. Diese Option wird nur dann in der Warnung angezeigt, wenn Personal Firewall zum Anzeigen von Empfehlungen konfiguriert wurde.

McAfee kennt möglicherweise das Programm nicht, das auf das Internet zuzugreifen versucht (Abbildung 4-6).

McAfee Personal Firewall Plus
Die Anwendung fordert Serverzugriff an.
Die Anwendung Server fordert an, als Server fungieren und eingehende Verbindungen annehmen zu können. Möchten Sie ihr Serverzugriff gewähren?
Pfad: C:\WINDOWS\Desktop\server.exe \Server.exe
McAfee...
erkennt diese Anwendung nicht.
Informieren Sie McAfee über dieses Programm.
Ich möchte...
Zugriff einmal gewähren
Serverzugriff gewähren
Auf abgehenden Zugriff beschränken
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 4-6. Warnung bei nicht unbekannter Anwendung

Deshalb kann McAfee auch keine Empfehlung geben, wie Sie mit dem Programm verfahren sollen. Sie können diese Anwendung an McAfee melden, indem Sie auf **Informieren Sie McAfee über dieses Programm** klicken. Es wird eine Webseite angezeigt, auf der Sie nach Informationen zum Programm gefragt werden. Übermitteln Sie bitte so viele Informationen wie möglich.

Mit den von Ihnen übermittelten Informationen versuchen unsere HackerWatch-Mitarbeiter mithilfe anderer Recherchetools festzustellen, ob ein Programm in unsere Anwendungsdatenbank aufgenommen werden soll, und wenn ja, wie Personal Firewall damit umgehen soll.

Zeigen Sie eine kurze Beschreibung des Ereignisses an, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten:

- Klicken Sie auf **Zugriff gewähren**, um der Anwendung ausgehende und eingehende Internetverbindungen zu erlauben.
- Klicken Sie auf **Zugriff einmal gewähren**, um der Anwendung eine vorübergehende Internetverbindung zu erlauben. Der Anwendung wird der Zugriff nur solange gewährt, bis sie wieder geschlossen wird.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um Internetverbindungen zu verbieten.
- Klicken Sie auf **Auf abgehenden Zugriff beschränken**, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).
- Klicken Sie auf **Hilfe bei der Auswahl**, um in der Onlinehilfe Informationen zu Zugriffsberechtigungen von Anwendungen abzurufen.

Warnung "Die Anwendung wurde geändert"

Wenn Sie in den **Sicherheitseinstellungen** die Option **Vertrauenswürdige**, **Standard** oder **Eingeschränkte** Sicherheit ausgewählt haben, zeigt Personal Firewall eine Warnung an (Abbildung 4-7), wenn es feststellt, dass eine Anwendung geändert wurde, der Sie bereits den Internetzugriff gewährt haben. Wenn Sie die fragliche Anwendung in letzter Zeit nicht aktualisiert haben, sollten Sie vorsichtig sein, wenn Sie ihr Zugriff auf das Internet gewähren.

McAfee Personal Firewall Plus
Die Anwendung wurde geändert
Die Anwendung Windows Media Player wurde geändert, seit Sie sie zum ersten Mal auf das Internet zugreifen ließen. Soll sie weiterhin Zugriff auf das Internet erhalten?
Pfad: C:\Programme\Windows Media Player\WMPLAYER.EXE
Ich möchte...
Zugriff gewähren
Zugriff einmal gewähren
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 4-7. Warnung "Die Anwendung wurde geändert"

Zeigen Sie eine kurze Beschreibung des Ereignisses an, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten:

- Klicken Sie auf **Zugriff gewähren**, um der Anwendung ausgehende und eingehende Internetverbindungen zu erlauben.
- Klicken Sie auf **Zugriff einmal gewähren**, um der Anwendung eine vorübergehende Internetverbindung zu erlauben. Der Anwendung wird der Zugriff nur solange gewährt, bis sie wieder geschlossen wird.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um Internetverbindungen zu verbieten.
- Klicken Sie auf **Abgehenden Zugriff gewähren**, um eine ausgehende Verbindung zuzulassen (**Eingeschränkte** Sicherheit).
- Klicken Sie auf **Hilfe bei der Auswahl**, um in der Onlinehilfe Informationen zu Zugriffsberechtigungen von Anwendungen abzurufen.

Warnung "Die Anwendung fordert Serverzugriff an"

Wenn Sie in den **Sicherheitseinstellungen** die Option **Eingeschränkte** Sicherheit ausgewählt haben, zeigt Personal Firewall eine Warnung an (Abbildung 4-8), wenn eine Anwendung, der Sie bereits den Zugriff auf das Internet gewährt haben, nun Internetzugriff als Server anfordert.

McAfee Personal Firewall Plus
Die Anwendung fordert Serverzugriff an.
Die Anwendung **Server** fordert an, als Server fungieren und eingehende Verbindungen annehmen zu können. Möchten Sie ihr Serverzugriff gewähren?
Pfad: C:\WINDOWS\Desktop\server.exe \Server.exe
Ich möchte...
Zugriff einmal gewähren
Serverzugriff gewähren
Auf abgehenden Zugriff beschränken
Gesamten Zugriff blockieren
Hilfe bei der Auswahl

Abbildung 4-8. Warnung "Die Anwendung fordert Serverzugriff an"

Beispielsweise wird eine Warnung eingeblendet, wenn MSN Messenger Serverzugriff anfordert, um während eines Chats eine Datei zu senden.

Zeigen Sie eine kurze Beschreibung des Ereignisses an, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten:

- Klicken Sie auf **Zugriff einmal gewähren**, um der Anwendung einen vorübergehenden Internetzugriff zu gewähren. Der Anwendung wird der Zugriff nur solange gewährt, bis sie wieder geschlossen wird.
- Klicken Sie auf **Serverzugriff gewähren**, um der Anwendung ausgehende und eingehende Internetverbindungen zu erlauben.
- Klicken Sie auf **Auf abgehenden Zugriff beschränken**, um eingehende Internetverbindungen zu verbieten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um Internetverbindungen zu verbieten.
- Klicken Sie auf **Hilfe bei der Auswahl**, um in der Onlinehilfe Informationen zu Zugriffsberechtigungen von Anwendungen abzurufen.

Grüne Warnungen

Grüne Warnungen benachrichtigen Sie bei Ereignissen in Personal Firewall, wenn beispielsweise einer Anwendung automatisch Internetzugriff gewährt wurde.

Programm darf auf das Internet zugreifen – Diese Warnung wird angezeigt, wenn Personal Firewall automatisch allen neuen Anwendungen Internetzugriff gewährt und Sie anschließend benachrichtigt (**Vertrauenswürdige** Sicherheit). Ein Beispiel für eine geänderte Anwendung ist eine Anwendung, deren Regeln geändert wurden, so dass der Anwendung nun automatisch der Internetzugriff erlaubt ist.

Warnung "Programm darf auf das Internet zugreifen"

Wenn Sie in den **Sicherheitseinstellungen** die Option **Vertrauenswürdige** Sicherheit ausgewählt haben, gewährt Personal Firewall automatisch allen neuen Anwendungen Internetzugriff und benachrichtigt Sie anschließend in Form einer Warnung (Abbildung 4-9).

McAfee Personal Firewall Plus
Programm darf auf das Internet zugreifen
Dem Programm MSN Messenger wurde automatisch Zugriff auf das Internet gewährt.
Pfad: C:\Programme\MSN Messenger \msnmsgr.exe
Anwendung erlaubt, weil...
McAfee diese Anwendung anerkennt.
Klicken Sie hier, um weitere Informationen anzuzeigen.
Ich möchte...
Anwendungsprotokoll anzeigen
Diesen Alarmtyp abschalten
Fortfahren

Abbildung 4-9. Programmdarf auf das Internet zugreifen

Zeigen Sie eine kurze Beschreibung des Ereignisses an, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten:

- Klicken Sie auf **Anwendungsprotokoll anzeigen**, um detaillierte Informationen zu dem Ereignis aus dem Internetanwendungsprotokoll anzuzeigen (siehe *Informationen zur Seite "Internetanwendungen"* auf Seite 101).
- Klicken Sie auf **Diesen Alarmtyp abschalten**, um das Anzeigen von Warnungen dieses Typs zu unterbinden.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um Internetverbindungen zu verbieten.

Warnung "Die Anwendung wurde geändert"

Wenn Sie in den **Sicherheitseinstellungen** die Option **Vertrauenswürdige** Sicherheit ausgewählt haben, gewährt Personal Firewall allen geänderten Anwendungen automatisch Internetzugriff. Zeigen Sie eine kurze Beschreibung des Ereignisses an, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten:

- Klicken Sie auf **Anwendungsprotokoll anzeigen**, um detaillierte Informationen zu dem Ereignis aus dem Internetanwendungsprotokoll anzuzeigen (siehe *Informationen zur Seite "Internetanwendungen"* auf Seite 101).
- Klicken Sie auf **Diesen Alarmtyp abschalten**, um das Anzeigen von Warnungen dieses Typs zu unterbinden.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.
- Klicken Sie auf **Gesamten Zugriff blockieren**, um Internetverbindungen zu verbieten.

Blaue Warnungen

Blaue Warnungen enthalten Informationen, es ist jedoch keine Reaktion Ihrerseits erforderlich.

- **Versuch, eine Verbindung herzustellen, wurde blockiert –** Diese Warnung wird angezeigt, wenn Personal Firewall unerwünschten Internet- oder Netzwerkverkehr blockiert. (**Vertrauenswürdige**, **Standard**- oder **Eingeschränkte** Sicherheit)

Warnung "Versuch, eine Verbindung herzustellen, wurde blockiert"

Wenn Sie die Sicherheitseinstellung **Vertrauenswürdige**, **Standard** oder **Eingeschränkte** Sicherheit ausgewählt haben, zeigt Personal Firewall eine Warnung an (Abbildung 4-10), wenn es unerwünschten Internet- oder Netzwerkverkehr blockiert.

McAfee Personal Firewall Plus
Versuch, eine Verbindung herzustellen, wurde blockiert
Ein Computer, mit dem Sie unter der IP-Adresse 192.168.1.40 kommuniziert haben, hat versucht, auf einen anderen als den erwarteten Anschluss (UDP Anschluss 1483) zuzugreifen.
Ich möchte...
Ereignisprotokoll anzeigen
Diese Adresse verfolgen
Diesen Alarmtyp abschalten
Fortfahren

Abbildung 4-10. Warnung "Versuch, eine Verbindung herzustellen, wurde blockiert"

Zeigen Sie eine kurze Beschreibung des Ereignisses an, und entscheiden Sie sich dann für eine der folgenden Möglichkeiten:

- Klicken Sie auf **Ereignisprotokoll anzeigen**, um detaillierte Informationen zu dem Ereignis aus dem Protokoll eingehender Ereignisse von Personal Firewall anzuzeigen (siehe *Informationen zur Seite "Eingehende Ereignisse"* auf Seite 103).
- Klicken Sie auf **Diese Adresse verfolgen**, um die IP-Adressen dieses Ereignisses visuell zu verfolgen.
- Klicken Sie auf **Diese Adresse sperren**, um zu verhindern, dass von dieser Adresse aus auf Ihren Computer zugegriffen wird. Die Adresse wird zur Liste **Gesperrte IP-Adressen** hinzugefügt.
- Klicken Sie auf **Diese Adresse als vertrauenswürdig einstufen**, um zu erlauben, dass von dieser Adresse aus auf Ihren Computer zugegriffen wird.
- Klicken Sie auf **Fortfahren**, wenn Sie keine zusätzlichen Maßnahmen ergreifen möchten.

Index

A

ActiveShield
- Aktivieren, 57
- Anhalten, 59
- Bereinigen eines Virus, 68
- Deaktivieren, 57
- Prüfen – nur Programmdateien und Dokumente, 65
- Prüfen aller Dateien, 64
- Prüfen aller Dateitypen, 64
- Prüfen auf neue, unbekannte Viren, 65
- Prüfen auf potenziell unerwünschte Programme (PUP), 67
- Prüfen auf Skripts, 65
- Prüfen auf Würmer, 61
- Prüfen der Anlagen von eingehenden Instant Messages, 63
- Prüfen von E-Mails und Anlagen, 59
- Prüfoptionen, 58
- Standardmäßige Scan-Einstellung, 59, 62 bis 67
- Starten, 59
- Testen, 54

Aktualisieren
- einer Rettungsdiskette, 84
- VirusScan
  - Automatisch, 87
  - Manuell, 87

Aktualisieren von Wireless Home Network Security
- Automatisches Prüfen auf Updates, 29
- Manuelles Prüfen auf Updates, 29

Alle Dateien überprüfen (Scan), 73

Anlagen von eingehenden Instant Messages
- Automatisch bereinigen, 63
- Prüfen, 63

Anzeigen von Ereignissen im Ereignisprotokoll, 107

Auf möglicherweise unerwünschte Programme überprüfen (empfohlen) (Scan), 74

Aufnehmen in die Positivliste
- PUP, 70

Automatische Windows-Updates, 116

AVERT, Übermitteln verdächtiger Dateien an, 81

B

Bearbeiten von Positivlisten, 71

C

Computer, schützen, 27

D

Deinstallieren
- anderer Firewalls, 91

E

Einrichten des Schreibschutzes für eine Rettungsdiskette, 83

Einstellungen, reparieren, 26

E-Mails und Anlagen
- Automatisch bereinigen
  - Aktivieren, 59
- Prüfen
  - Aktivieren, 59
  - Deaktivieren, 61
  - Fehler, 60

Ereignisprotokoll
- Anzeigen, 113
- Info, 103
- Verwalten, 113

Ereignisse
Anzeigen
alle, 107
aus dieser Woche, 107
eines bestimmten Tages, 108
heutige, 107
mit identischen Ereignisinformationen, 108
von bestimmter Adresse, 108
Archivieren des Ereignisprotokolls, 113
Exportieren, 114
Hinweise von HackerWatch.org, 109
Info, 103
Kopieren, 114
Loopback, 105
Löschen, 114
Löschen des Ereignisprotokollinhalts, 114
Melden, 110
Reagieren auf, 109
Verfolgen
Anzeigen von archivierten Ereignisprotokollen, 113
Grundlegendes, 103
von 0.0.0.0, 105
von 127.0.0.1, 105
von Computern in Ihrem lokalen Netzwerk (LAN), 106
von privaten IP-Adressen, 106
Weitere Informationen, 109
Ereignisse, anzeigen, 24
Erste Schritte mit VirusScan, 53
Erstellen einer Rettungsdiskette, 82
Erweiterte Einstellungen
Sicherheit, 24
Warnungen, 25
Weitere, 25

F

Funktionen, 16
Funktionen, neue, 53, 89

H

HackerWatch.org
Anmelden, 110
Empfehlungen, 109
Melden eines Ereignisses an, 110

I

Internetanwendungen
Ändern von Anwendungsregeln, 102
Info, 101
Zulassen und Blockieren, 102
IP-Adressen
Info, 104
Sperren, 111
Vertrauen, 110

K

Komprimierte Dateien überprüfen (Scan), 73
Konfigurationsassistent, verwenden, 18
Konfigurieren
VirusScan
ActiveShield, 57
Scan, 71

L

Liste der entdeckten Dateien (Scan), 75, 79
Liste der vertrauenswürdigen PUPs, 71

M

McAfee SecurityCenter, 11
Melden eines Ereignisses, 110
Microsoft Outlook, 76

N

Nach neuen, unbekannten Viren scannen (Scan), 74
Netzwerk
Anzeigen, 20
Aufheben des Schutzes, 28
Schützen, 28
Trennen, 22
Verbinden, 22
Widerrufen des Zugriffs, 26

O

Optionen
- Erweitert, 22
- Konfigurieren, 23

Optionen (Seite), 23
Optionen, konfigurieren, 23

P

Personal Firewall
- Testen, 95
- Verwenden, 95

Planen von Scanvorgängen, 76
Potenziell unerwünschte Programme (PUP), 67
- Bereinigen, 79
- Entfernen, 70
- Erkennen, 78
- Isolieren, 79
- Löschen, 79
- Vertrauen, 70
- Warnungen, 70

Problembehandlung, 33
Programme in der Positivliste, 71
Prüfen
- alle Dateien, 64, 73
- auf neue, unbekannte Viren, 74
- auf potenziell unerwünschte Programme (PUP), 67
- auf Skripts, 65
- auf Würmer, 61
- Komprimierte Dateien, 73
- nur Programmdateien und Dokumente, 65
- per Windows Explorer, 76
- Planen automatischer Scanvorgänge, 76
- über die Microsoft Outlook-Symbolleiste, 76
- Unterordner, 72

Prüfoptionen
- ActiveShield, 58, 64 bis 65
- Scan, 71

Q

Quarantäne
- Bereinigen von Dateien, 80 bis 81
- Hinzufügen verdächtiger Dateien, 80
- Löschen verdächtiger Dateien, 81
- Löschen von Dateien, 80
- Übermitteln verdächtiger Dateien, 81
- Verwalten verdächtiger Dateien, 80
- Wiederherstellen von bereinigten Dateien, 80 bis 81

R

Rettungsdiskette
- Aktualisieren, 84
- Erstellen, 82
- Schreibschutz einrichten, 83
- Verwenden, 79, 83

S

Scan
- Alle Dateien überprüfen (Option), 73
- Auf möglicherweise unerwünschte Programme überprüfen (empfohlen) (Option), 74
- Automatisches Überprüfen, 76
- Bereinigen eines Virus oder eines potenziell unerwünschten Programms, 79
- Isolieren einen Virus oder eines potenziell unerwünschten Programms, 79
- Komprimierte Dateien überprüfen (Option), 73
- Löschen eines Virus oder eines potenziell unerwünschten Programms, 79
- Manuelles Prüfen, 71
- Manuelles Prüfen per Windows Explorer, 76
- Manuelles Prüfen über die Microsoft Outlook-Symbolleiste, 76
- Nach neuen, unbekannten Viren scannen (Option), 74
- Testen, 55 bis 56
- Unterordner überprüfen (Option), 72

Schlüssel, rotieren, 28
Schnellreferenz, iii
ScriptStopper, 65

Skripts
Anhalten, 69
Warnungen, 69
Zulassen, 69
Standard-Firewall, Festlegen der, 92
Systemanforderungen, 9

T

Technischer Support, 79
Testen von Personal Firewall, 95
Testen von VirusScan, 54
Trojaner
Erkennen, 78
Warnungen, 68

U

Übermitteln verdächtiger Dateien an AVERT, 81
Unterordner überprüfen (Scan), 72
Update-Assistent, 58

V

Verbindung, anzeigen, 19
Verfolgen eines Ereignisses, 109
Verfügbare drahtlose Netzwerke (Seite), 21
Verwenden einer Rettungsdiskette, 83
Viren
Anhalten potenzieller Würmer, 69
Anhalten verdächtiger Skripts, 69
Automatisch melden, 84, 86
Bereinigen, 68, 78
Entfernen von PUPs, 70
Erkennen, 78
Erkennen mit ActiveShield, 68
Isolieren, 68, 78
Isolieren entdeckter Dateien, 68
Löschen, 68, 78
Löschen entdeckter Dateien, 69
Warnungen, 68
Zulassen verdächtiger Skripts, 69
VirusScan
Automatisches Aktualisieren, 87
Automatisches Melden von Viren, 84, 86
Erste Schritte, 53
Manuelles Aktualisieren, 87
Planen von Scanvorgängen, 76
Prüfen per Windows Explorer, 76
Prüfen über die Microsoft Outlook-Symbolleiste, 76
Testen, 54

W

Warnungen, 30
bei entdeckten Dateien, 68
bei entdeckten E-Mails, 69
bei potenziellen Würmern, 69
bei PUPs, 70
bei verdächtigen Skripts, 69
bei Viren, 68
Die Anwendung fordert Serverzugriff an, 116
Die Anwendung möchte auf das Internet zugreifen, 115
Die Anwendung wurde geändert, 115
Internetanwendung blockiert, 115
Neu zugelassene Anwendung, 121
Versuch, eine Verbindung herzustellen, wurde blockiert, 122
Windows Explorer, 76
Windows-Firewall, 92
Wireless Home Network Security
Einführung, 14
Verwenden, 13
World Virus Map
Anzeigen, 86
Melden, 84
WormStopper, 61
Würmer
Anhalten, 69
Erkennen, 68, 78
Warnungen, 68 bis 69

Z

Zusammenfassung (Seite), 19, 21, 95